Comparative Review: Disk Imaging p. 19 ■ Top 10 Virtual Server Tips p. 77

MANAGEMENT • SECURITY • NETWORKING • MESSAGING • HOW-TO

Windows® IT Pro

Connecting the IT Community

EVERYDAY IT ANNOYANCES

- File and Print Problems p. 26
- Group Policy Gotchas p. 32
- DNS Dilemmas p. 35
- Security Snags p. 39

REQUIRED READING

- Exchange Storage and Compliance p. 45
- Disaster Preparedness Checklist p. 49
- Perimeter Security p. 53

SharePoint & Office Pro

- Site Security p. 57
- MOSS Unleashed p. 62
- Office Servers Explained p. 65

Penton
A PENTON PUBLICATION
FEBRUARY 2007
WWW.WINDOWSITPRO.COM
U.S. $5.95 CANADA $7.95

Windows IT Pro

FEBRUARY 2007 VOLUME 13 NO. 2

COVER STORY

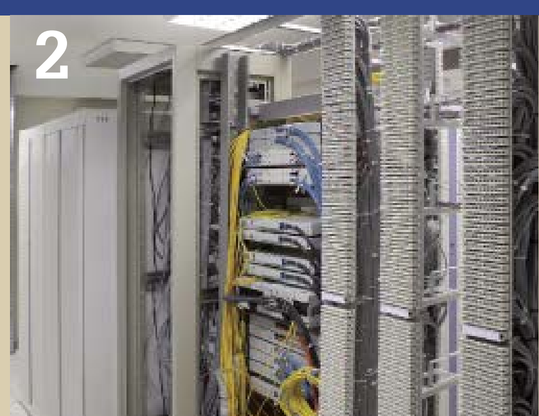
EVERYDAY IT ANNOYANCES

FEATURES

SHAREPOINT & OFFICE PRO

COLUMNS

Access articles online at http://www.windowsitpro.com. Enter the article ID in the InstantDoc ID text box.



PRODUCTS

12

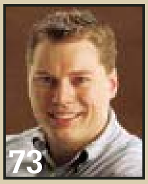
14

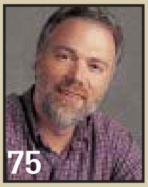
14

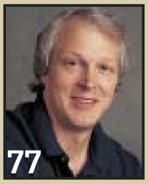
—Carlton Whitmore, systems analyst

WHAT'S HOT

IN EVERY ISSUE



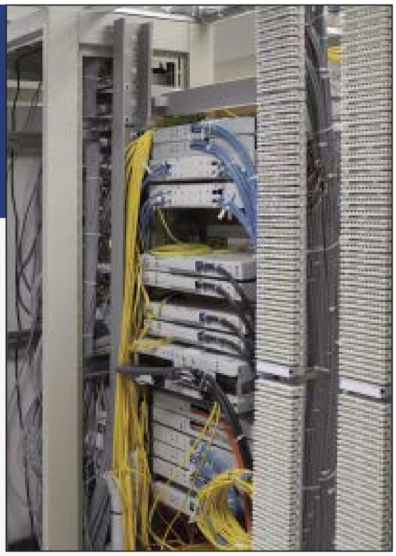




Learning Path Article not a perfect fit? Find more resources to match your knowledge and skills.
Interact! Network with authors, peers, product vendors, and Microsoft.

windowsitpro.com

THE MORE, THE MESSIER:
MANAGING MULTIPLE SYSTEMS



"Server Consolidation Essentials"

Discover the benefits of using virtualization technologies to consolidate your servers. The first chapter of this free eBook is available now and includes details about how server consolidation can help you do more with less.

http://www.windowsitpro.com/go/ebooks/microsoft/consolidation

"Evidence Mapping: An Innovative Approach to Demonstrating Multi-Regulatory Compliance"

In this free on-demand Web seminar, learn to gather evidence of compliance across multiple systems and link the data to regulatory and framework control objectives.

http://www.windowsitpro.com/go/seminars/bindview/multiregcompliance

"Email Is Down: Now You're Out of Compliance!"

When your email systems go down, your employees find alternate communication methods—which may not be compliant with your messaging regulations. Download this free Executive Guide and discover the effect of email outages on compliance and learn methods for establishing continuity in your corporate messaging environment.

http://www.windowsitpro.com/go/whitepapers/messageone/continuity

Your Savvy Assistant

Let your new assistant gather information and pull together resources you might not be aware of. Check out this Web-exclusive column, which points you to the hottest articles in systems management, messaging, SharePoint, Office, networking and hardware, security, and SQL Server.

http://windowsitpro.com/departments/departmentid/1035/1035.html

Longhorn Is Coming—Get In on the Ground Floor

Here's your chance to preview Longhorn, interact with Longhorn experts, and provide product feedback to Microsoft. The Longhorn roadshow series is visiting 16 US cities in March, April, and May. The roadshows will feature local "ChampFest" IT trivia contests, and local contest winners have the opportunity to compete at Fall Connections in Las Vegas!

http://www.windowsitpro.com/go/longhornshows

TechX World 2007: Interoperability in Depth

Virtualization, user identities, network management, OS management: Wouldn't life be nice if all core technologies fit together perfectly? TechX World 2007 addresses these topics and more, teaching IT pros to effectively manage interoperability. Join TechX World in San Francisco, New York City, or Washington DC, this spring. Register now!

http://www.windowsitpro.com/go/techx

TECHXWORLD

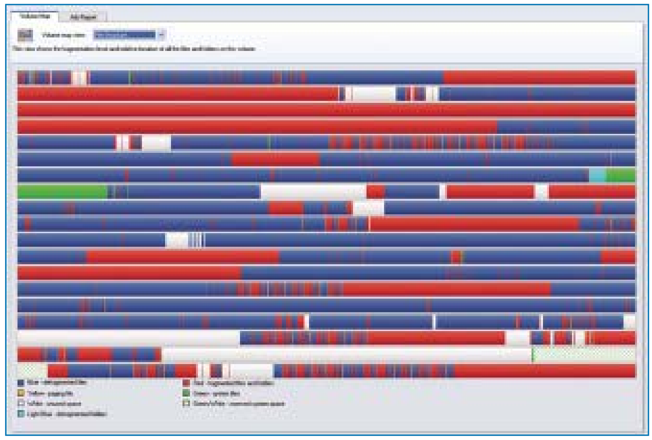
Don't Be Just a Pro, Be a Pro VIP

As a Pro VIP member, you'll have access to the same great technical articles that have been the hallmark of *Windows IT Security, Windows Scripting Solutions*, and *Exchange & Outlook Administrator*. Membership benefits include weekly email messages or RSS notifications linking to a new online article; a monthly email newsletter that includes a commentary from the editor and a printable version of recent online articles; access to the Pro VIP Web sites and members-only forums; and the *Windows IT Security, Windows Scripting Solutions*, and *Exchange & Outlook Administrator* article archives.

http://www.securityprovip.com, http://www.exchangeprovip.com, and http://www.scriptingprovip.com

Restore and Maintain Peak Performance

Eight things you need to know – a special report



Diskeeper's interface shows fragmentation levels and relative location of all the files and folders on the selected volume.

As an IT Professional, you know the importance of maintaining system performance and reliability. Your team is the one called to the rescue when desktops or servers crash, slow down or freeze. Many of these issues stem from a single, hidden source: disk fragmentation.

1. Reliability issues commonly traced to disk fragmentation: Crashes and system hangs/freezes; slow boot times and boot failures; slow back up times and aborted backup; file corruption and data loss; errors in programs; cache issues; hard drive failures.

Having files stored contiguously on the hard drive is a key factor in keeping a system stable and performing at peak efficiency. Even a small amount of fragmentation in your most used files can lead to crashes, conflicts and errors.

2. The weak link in today's computers: A computer system is only as fast as its slowest component. The disk drive is by far the slowest of the three main components of your computer: CPU, memory and disk. Even with the fastest CPU system performance would be affected by disk fragmentation.

3. Is real-time, automatic defragmentation needed in today's environment? More than ever! Large disks, multimedia files, applications, operating systems, system up-dates, virus signatures — all dramatically increase the rate of fragmentation. Fragmentation increases the time to access files for all common system activities including opening and closing Microsoft® Word documents, searching for emails, opening web pages and performing virus scans. To keep performance at peak, fragmentation must be eliminated instantly.

4. Increased server uptime: Fragmentation can cripple server performance and reliability resulting in downtime and lost production. Diskeeper can easily and safely be used on your servers including: file and print, web, domain controllers, SQL, Exchange, and any other database or application servers.

5. Virtualization and fragmentation: Server virtualization can be used to reduce the number of physical systems for more efficient CPU utilization. However, there is a downside; the disk subsystem must now account for increased disk I/O. Disk fragmentation is the primary cause of unnecessary I/O overhead. Automatic defragmentation is more important than ever for maximum performance.

6. Hidden scheduled defragmentation costs: Scheduled defragmentation is not "free" — it has heavy hidden costs, such as IT time to set and monitor defrag for every system. This results in either staying after hours to defrag, giving the users administrator privileges (not likely!), break-fix handlings, or more often *no defrag whatsoever*.

7. How do I find out how much fragmentation I have? Download a free trial version of new Diskeeper 2007 at:

www.diskeeper.com/winitpro

Install it, select a volume, select Analyze and view the report.

8. Advanced, automated defragmentation: Maintaining systems can be a daunting task - maintenance, including regular defragmentation, must take place regularly to keep them running at peak levels. However, with constant uptime required, scheduling such processes to run at the right times can be tricky, since while running they pose a considerable drain on system resources.

Diskeeper 2007 marks the end of scheduling, and the beginning of REAL TIME, on the fly maintenance of systems. Never again worry about dips in performance or straining valuable system resources - even when demand is at its absolute highest!

Customers agree Diskeeper maintains the performance and reliability of their desktops and servers, reducing maintenance and increasing hardware life.

Every system you manage needs Diskeeper for enhanced file system performance — automatically!

Diskeeper® 2007
Enhancing File System Performance
— *Automatically™*

Special Offer

Try Diskeeper 2007 FREE for 45 days!
Download: www.diskeeper.com/winitpro
(Note: Special 45-day trialware is only available at the above link)

Volume licensing and Government / Education discounts are available from your favorite reseller or call 800-829-6468 code 9250

For test results, white papers and case studies, visit http://www.diskeeper.com/winitprodocs

Diskeeper® corporation

Searching for Microsoft Vista Management Products?
Microsoft GOLD CERTIFIED Partner
CERTIFIED FOR Windows Vista™

Where's the Wow Over Exchange 2007?

Preaching to the choir keeps the choir singing

Exchange admins are a loyal bunch, as witnessed by the fact that the Exchange community remains cohesive despite what sometimes seems like Microsoft's best efforts to discourage it. For example, back in the 1990s, the annual Microsoft Exchange Conference (MEC) was a highly successful gathering of Exchange enthusiasts. These dedicated professionals enjoyed getting together with Microsoft and learning from each other. But in the wake of the tech crash, Microsoft consolidated its conferences and rolled MEC into TechEd. Too bad, Exchange community: You've been assimilated into an all-encompassing IT assembly and the focus on Exchange has been dispersed. However, not to be discouraged so easily, this resilient group has rallied around the Exchange Connections conference and kept the spirit growing. That's what I call bonding with a technology.

Considering Microsoft's focus on IT community in the past few years, you'd think the company would be holding up Exchange as a shining model of customer engagement. Here's an organic, thriving, and authentic community that persists because people identify with the product, not because Microsoft has decided community is the answer to poor customer satisfaction.

Keep the Choir Singing

Just when I think Microsoft gets the idea of customer service and community, the company decides it can take an enthusiastic group of customers for granted in order to steer them toward a shiny new technology. Dismal IT customer satisfaction resulted when Microsoft dropped Windows NT devotees like hot potatoes after the launch of Windows 2000 (Win2K). The company's attitude seemed to be, "If we build Win2K, IT will come." Back in those days, I can't tell you how often I heard Microsoft say the company didn't need to waste time "preaching to the choir."

The launch of Windows Vista, Office 2007, and—oh, yeah—Exchange 2007 gives me the feeling that Microsoft is once again testing the resolve of the Exchange community. It seems the company just expects Exchange users to jump on the Exchange 2007 bandwagon, so there's no need to celebrate the launch and the community's responsibility for Exchange's success. More significantly, though, Office Communications Server (OCS, the successor to Live Communications Server—LCS), which is the company's strategic priority, is scheduled for launch by mid-2007 and it seems that Microsoft is trying to shift the focus away from Exchange to OCS, the enabler of the company's new Unified Communications (UC) effort.

Think Like Your Customers

Of course, focusing on UC as a way to get IT excited about a new direction is absolutely appropriate and points to an evolutionary change in how people will be able to communicate efficiently. I just think Microsoft's long-term strategy for UC is clouding its judgment about the importance of keeping Exchange enthusiasts engaged and excited along the way.

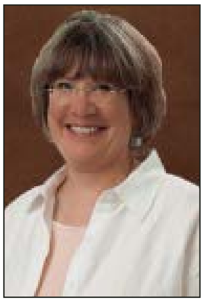
But more important, I believe this lack of consideration for IT is connected to Microsoft's moving Exchange, a server product that used to be part of the Server and Tools Division, into the company's Office business unit. The company has always considered Office an end-user product—the Office division's name is Information Worker Business Unit (IWBU). Although the Office team does an outstanding job of serving information workers' needs, I haven't noticed the team investing much effort in understanding IT customer satisfaction. In fact, I've been shocked at the arrogance of some Office representatives when I've tried to talk to them about the issues that are of importance to IT. But the Office group has always considered itself fairly unassailable in its dominance of the desktop, so it makes sense that this attitude would transfer to new members of the Office family.

Celebrating, Not Relegating

The good news is that Microsoft people who have been associated with Exchange since before the organizational move do understand IT's needs. Evidence of their commitment to the Exchange community is a series of local events starting in March under the title *Microsoft Unified Communications: Featuring Exchange Server 2007* and cosponsored by this publication and Microsoft (http://www.windowsitpro.com/roadshows/exhange2007usa). Although these events fall under the umbrella of UC, the focus will be on core IT considerations: Exchange 2007 architecture, deployment, management, security, and mobility. These events will provide an IT context and demonstrate how Exchange fits into the bigger picture of UC.

If the IWBU doesn't want to test the strong loyalty of Exchange admins yet again, the division needs to get attuned to the IT folks who are and will continue to be responsible for Exchange—not to mention OCS. It would be a shame to start hearing again that Microsoft doesn't need to preach to the IT choir. Even if no highly attractive alternatives to Exchange are available to tempt current customers, neglecting a vital community is never a good idea.

InstantDoc ID 94764



Karen Forster
(karen@windowsitpro.com) is editorial and strategy director for *Windows IT Pro* and *SQL Server Magazine* and former director of Windows Server User Assistance at Microsoft.

Did You Know?

Are you ready to tackle Exchange 2007? Co-located with Office Connections 2007 and Windows Connections 2007 in Orlando in April, the Microsoft Exchange Connections 2007conference will bring you up to speed on Exchange 2007's new security, administration, and unified messaging features (http://www.devconnections.com/shows/SP2007EXCH/default.asp?s=94).

EDITORIAL

Editorial and Strategy Director
Karen Forster karen@windowsitpro.com

Executive Editor
Amy Eisenberg amy@windowsitpro.com

Technical Director
Michael Otey mikeo@windowsitpro.com

Senior Technical Editor
Diana May dmay@sqlmag.com

Systems Management
Barb Gibbens Deputy Editor bgibbens@windowsitpro.com
Karen Bemowski Senior Editor kbemowski@windowsitpro.com
Caroline Marwitz Associate Editor cmarwitz@windowsitpro.com

Messaging , SharePoint, and Office
Anne Grubb Senior Editor agrubb@windowsitpro.com
Gayle Rodcay Senior Editor grodcay@windowsitpro.com
Brian Winstead Assistant Editor bwinstead@windowsitpro.com

Networking and Hardware
Jason Bovberg Senior Editor jbovberg@windowsitpro.com
Megan Bearly Assistant Editor mbearly@windowsitpro.com

Security
Renee Munshi Senior Editor rmunshi@windowsitpro.com

SQL Server
Dawn Cyr Senior Editor dcyr@sqlmag.com

Production Editor
Christan Humphries chumphries@windowsitpro.com

Administrative Assistant
Mary Waterloo mwaterloo@windowsitpro.com

News Editor
Paul Thurrott news@windowsitpro.com

Senior Contributing Editors
David Chernicoff david@windowsitpro.com
Mark Joseph Edwards mje@windowsitpro.com
Kathy Ivens kivens@windowsitpro.com
Mark Minasi mark@minasi.com
Mark Russinovich mark@sysinternals.com

Contributing Editors
Bob Chronister bob@windowsitpro.com
Jerry Cochran jerryco@microsoft.com
Sean Deuby sdeuby@windowsitpro.com
Jeff Fellinge jeff@blackstatic.com
Brett Hill brett@iisanswers.com
Dan Holme danh@intelliem.com
Darren Mar-Elia dmarelia@windowsitpro.com
Sue Mosher exadmin@turtleflock.com
Tony Redmond tony.redmond@hp.com
Paul Robichaux paul@robichaux.net
Ed Roth eroth@windowsitpro.com
William Sheldon bsheldon@interknowlogy.com
Randy Franklin Smith rsmith@montereytechgroup.com
Orin Thomas orin@windowsitpro.com
Douglas Toombs help@toombs.us
Ethan Wilansky ewilansky@windowsitpro.com

PRODUCTS & REVIEWS

Senior Editor, Products
Dianne Russell drussell@windowsitpro.com

Product Editor
Blake Eno beno@windowsitpro.com

Editorial Assistant
Sam Davenport sdavenport@windowsitpro.com

ART & PRODUCTION

Senior Art Director
Larry Purvis lpurvis@windowsitpro.com

Art Director
Layne Petersen layne@windowsitpro.com

Production Director
Linda Kirchgesler linda@windowsitpro.com

Senior Production Manager
Kate Brown kbrown@windowsitpro.com

Assistant Production Manager
Erik Lodermeier elodermeier@penton.com

Production Assistant
Tina Parker tparker@penton.com

CUSTOM MEDIA

Custom Director and SQL Server Business Manager
Michele Crockett mcrockett@windowsitpro.com 970-203-2924

Group Editorial Director
Dave Bernard dbernard@windowsitpro.com

Penton
Penton Media, Inc.

David B. Nussbaum **Chief Executive Officer**
Preston L. Vice **Chief Financial Officer & Corporate Secretary**
James Ogle **Vice President, Finance**
Colleen Zelina **Sr. Vice President, Human Resources & Organizational Effectiveness**
Eric Shanfelt eshanfelt@penton.com **Sr. Vice President, eMedia Strategy & Development**
Darrell C. Denny ddenny@penton.com **President, IT, Lifestyle, Food/Retail Media Groups**

WRITING FOR WINDOWS IT PRO
Submit queries about topics of importance to Windows managers and systems administrators to articles@windowsitpro.com.

PROGRAM CODE

SUBSCRIPTION INFORMATION
Subscriptions in US, $49.95 for one year (12 issues for 2007); in-Canada, $59 US currency, plus 7% for GST for-one year; in UK £59; in all other countries, US $99. Payment should be made in US dollars drawn on US banks. For new subscriptions,-call 800-793-5697 or 970-663-4700, or check our Web site at http://www.windowsitpro.com. For questions or other subscription problems, call customer service at 800-793-5697 or email subs@windowsitpro.com. Europe, europe@windowsitpro.com, *Windows IT Pro,* Di-An House, 2 Aegean Road, Atlantic Street, Altrincham, Cheshire, WA14 5UW, England; tel.-0161 929 2800, fax-0161 929 1511.

Group Publisher
Kim Paulsen kpaulsen@windowsitpro.com

Group Administrative Manager
Danna Varnell dvarnell@windowsitpro.com

Associate Publisher
Peg Miller pmiller@windowsitpro.com

National Sales Manager
Jeff Lewis jlewis@windowsitpro.com 970-613-4960

eMedia Strategist
Chad Phelps cphelps@windowsitpro.com 970-203-2690

ADVERTISING SALES

Northwest Sales Manager
Jeff Carnes jcarnes@windowsitpro.com 678-455-6146

Northwest Account Executive
Kristi Kelley kkelley@windowsitpro.com 970-203-2818

Southwest Sales Manager
Chrissy Kontras ckontras@windowsitpro.com 970-203-2883

Southwest Account Executive
Scott Eastman seastman@windowsitpro.com 970-613-4922

Eastern Sales Manager
Lisa Rogers lrogers@windowsitpro.com 404-355-7494

Eastern Account Executive
Doug Hay dhay@windowsitpro.com 970-613-4931

Southwest and Eastern Client Services Manager
Karen Shaw-Lafferty kshaw@windowsitpro.com 970-203-2967

Northwest Client Services Manager
Michelle Andrews mandrews@pentontech.com 970-613-4964

Ad Production Supervisor
Glenda Vaught gvaught@pentontech.com

REPRINTS

Reprint Sales
Michael Dudziak mdudziak@penton.com 216-931-9324 888-858-8851

MARKETING & CIRCULATION

Circulation Manager
Marie Evans mevans@penton.com

Direct Marketing Manager
Katie Buel kbuel@penton.com

eMedia Circulation Marketing Manager
Christina Ross cross@windowsitpro.com

Renewal Marketing Manager
Tricia McConnell tricia@windowsitpro.com

EMEA Circulation Marketing Manager
Irene Clapham irene@windowsitpro.com

Strategic Marketing Manager
Demian Straka dstraka@windowsitpro.com

Marketing Associates
Brandi Johnson bjohnson@windowsitpro.com
Amy Reitz areitz@windowsitpro.com

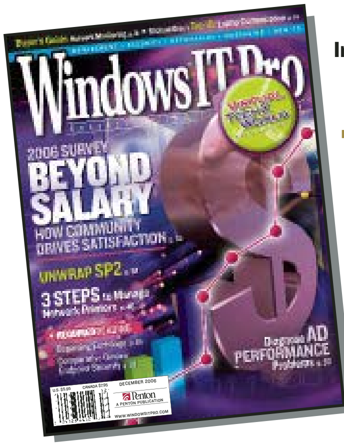
Correcting Inaccuracies About DeviceLock

In the December 2006 issue of *Windows IT Pro*, SmartLine's DeviceLock 6.0 was included in the comparative product review "Client Device Managers" (InstantDoc ID 93926). The reviewer, Karl D. Middlebrooks, made claims about DeviceLock that are incorrect. We'd like to set the record straight for *Windows IT Pro*'s readers and our customers.

Mr. Middlebrooks wrote, "Unfortunately, DeviceLock provides no out-of-the-box way to produce reports on the logging data, so a third-party reporting utility is required to make the best use of the audit trail." This statement and the row in the article's product feature table that indicates DeviceLock does not include reporting tools are incorrect. Through the DeviceLock Enterprise Manager (DLEM) console that is installed by default, DeviceLock has several obvious "out-of-the-box" reporting tools and doesn't require third-party solutions. In version 6.0, which was reviewed in the article, the following enterprise reporting tools are easily accessible:

- Permissions reports, for determining access and audit policy settings on managed endpoint computers.
- Audit Log Viewer reports (with sorting and wildcard filtering by column), for working with standard logging DeviceLock data from managed endpoint computers.
- Plug 'n' Play Auditor reports, for determining what USB, FireWire, and PCMCIA devices have been or currently are installed on endpoint computers. This report can also be used to populate the USB White List database.
- Shadow Log Viewer reports (with sorting and wildcard filtering by column), for working with DeviceLock Data Shadow logs from managed endpoint computers.

Pricing plays a major role in the decision to purchase any product. Unfortunately, the pricing listed for DeviceLock in the article is incorrect and represented only the purchase of a single DeviceLock license—which retails for $35.00 per computer—whereas the two competing products were compared at volume pricing for 25 licenses—respectively, $25.00 and $27.50 per computer. DeviceLock's volume pricing for 25 licenses is $22.00 per computer. Volume pricing for 100 seats is $15.50 per computer, and pricing for 1,000 seats is $7.40 per computer. DeviceLock's volume pricing information is available at http://www.devicelock.com.



Mr. Middlebrooks stated that only Centennial Software's DeviceWall 4.0 has a "Deny Permission" feature. In fact, DeviceLock's permission parameter is called NO ACCESS and performs the same function. DeviceLock also provides a Read-Only permission parameter for ports and devices that can store files.

Finally, Mr. Middlebrooks reported that DeviceLock doesn't use the grouping of computers for policy settings. It's true that DeviceLock doesn't use any foreign constructs or database abstracts of the environment as other solutions do to "artificially group" computers. However, through the DeviceLock Enterprise Manager console, an administrator can leverage native directory structures and containers to represent "Groups of Computers" to list and select for similar policies, such as "Organizational Units (OUs)," "Computer Types," "LDAP OUs," and/or importing computer names from a set list. Administrators can also choose to multiselect any desired computers from a domain container or network list.

Like many of you, we believe that *Windows IT Pro* continues to be a highly respected, trusted news source for our industry. We appreciate the opportunity to set the record straight about DeviceLock.

—Chris Heinemann
Manager, Marketing Communications,
AdvancedForce InfoSecurity Solutions, Inc.

The Value of Vista

Regarding Karen Forster's IT Pro Perspective: "The Value of Vista, Office, and Exchange" (January 2007, InstantDoc ID 94455), I'm the network admin for a small college in Wisconsin, and I can tell you that we're not planning to move to Vista any time soon. Heck, we're only grudgingly considering 64-bit upgrades to our OSs. The big problems: hardware upgrade costs and software incompatibility. For example, we can't easily afford to migrate off Windows Messenger 5.1, which is incompatible with Vista. Moreover, many of the basic Windows Server 2003 admin tools don't run properly on Vista (or on 64-bit systems)—which is, by the way, a lack of professional polish that I consider unacceptable. Although members of our staff have gotten the admin pack and other tools to run on Vista by manually registering DLLs and coyping a few files manually into different system folders, my belief is that Microsoft—which presumably wants our business—should be offering Vista-compatible tools right off the bat. After all, IT departments are the early adopters; if we're just going to use remote desktop to connect to another workstation to do our basic administrative tasks (as Microsoft workarounds suggest), what value is there in Vista to us?

—Tom Davidson

InstantDoc ID 94834

EDITOR'S NOTE

Windows IT Pro welcomes feedback about the magazine. Send comments to letters@windowsitpro.com, and include your full name, email address, and daytime phone number. We edit all letters and replies for style, length, and clarity.

Oops

The article "Windows SharePoint Services 3.0 Out of the Box" (January 2007, InstantDoc ID 94240) referenced a URL that is not yet active. The URL should be http://www.MyMSOfficePro.com. Check back soon for details. We apologize for any inconvenience this error might have caused.

What You Need to Know About ...

Kernel Patch Protection

Paul Thurrott
(thurrott@windowsitpro.com) is the news editor for *Windows IT Pro*. He writes a weekly editorial for *Windows IT Pro UPDATE* (http://www.windowsitpro.com/email) and a daily Windows news and information newsletter called *WinInfo Daily UPDATE* (http://www.wininformant.com).

An esoteric security feature in Windows Vista called Kernel Patch Protection (aka PatchGuard) garnered a lot of attention after security software companies complained that Microsoft was using the feature to shut them out of the new OS. Kernel Patch Protection is widely misunderstood, and security companies have certainly misrepresented the feature to the public. Here's what you need to know about Kernel Patch Protection.

First, It's 64-Bit Only

The most often misunderstood fact about Kernel Patch Protection is that the feature is present only in Vista x64 editions, including the 64-bit editions of Vista Home Premium, Vista Business, Vista Enterprise, and Vista Ultimate. Kernel Patch Protection isn't present in the more mainstream 32-bit versions of Vista.

What It Does

Kernel Patch Protection prevents what has become a common practice with Windows XP: Both malicious hackers and security firms have come to rely on the ability to patch (or "hook") the Windows kernel at runtime. This practice can lead to system instability because the kernel is the core component of the Windows OS and is used by all other OS components, applications, and services. Of all the malicious software that relies on kernel patching to infiltrate Windows, probably the most common type is the so-called rootkit, which is often impossible to remove because of its deep hooks in the Windows kernel.

Security software firms began using kernel-patching techniques years ago to battle these new, more malicious forms of malware. But any kernel patch, malicious or otherwise, can render a Windows system unstable and generate a blue screen. The result is a nasty crash.

In 32-bit versions of Vista, the kernel behaves much like it does in XP, and security software firms can continue patching the 32-bit Vista kernel at runtime, helping reduce instances of rootkits and other malicious software. But in 64-bit versions of Vista, Kernel Patch Protection renders this practice obsolete. Kernel Patch Protection—which debuted in XP Professional x64 Edition and the 64-bit versions of Windows Server 2003 with Service Pack 1 (SP1)—prevents the Windows kernel from being patched at runtime. When Kernel Patch Protection detects an attempt to patch the kernel, it immediately shuts down the OS.

An immediate shutdown might sound like an overly severe reaction, but Microsoft says it's by design. The idea is to prevent the kernel from being modified, and to do that, Kernel Patch Protection has to shut down the OS; otherwise, hackers might be able to inject malicious code into the kernel while the user is fumbling with consent dialog boxes.

As its name suggests, Kernel Patch Protection protects only the kernel. It isn't designed to be a general tool for preventing malware or attacks on other parts of the OS. Of course, Vista includes other security technologies, such as Address Space Layout Randomizer and Windows Defender, that provide a baseline level of support against other kinds of malware.

The Complaints

Companies such as McAfee and Symantec, which have built successful businesses by protecting individuals and businesses against the electronic threats that endanger Windows systems, have complained that Kernel Patch Protection prevents them from providing the same types of protections for Vista that they provided for XP. Microsoft counter-argued that Kernel Patch Protection makes 64-bit Vista versions more secure and stable and renders kernel patching by security companies unnecessary and obsolete.

In the days before Vista was finalized, however, Microsoft announced a compromise: It will create a set of APIs that will enable security software firms to interact with Kernel Patch Protection at a programmatic level, providing them with at least some of the kernel patching functionality they've requested. Microsoft says it will deliver these APIs in late 2007, perhaps as part of Vista SP1, which is due out at the same time as Longhorn Server.

This timetable has generated a second round of complaints from security firms, which argue that the wait is too long. However, x64 uptake won't pick up in the first year of Vista availability. Although it's likely that most Vista users will move to x64 systems in the future, that transition will take years. In the meantime, users of Vista 64-bit editions will be safer with Kernel Patch Protection in place.

Recommendations

Kernel Patch Protection is a valuable addition to Vista and will make Vista more secure and stable. Any complaints about this functionality on the part of security software firms is political posturing: Because of Microsoft's numerous antitrust problems around the world, these companies believe they can threaten Microsoft and find a friendly ear with regulatory bodies in various countries.

InstantDoc ID 94219


_INFRASTRUCTURE LOG
_DAY 44: This lack of productivity is out of control. What we're using isn't working. Gil's had enough. He moved everyone into one cubicle. A "collaboration" cubicle. We need a better idea.
_DAY 46: I'm going with IBM Lotus® Notes® and Domino®. It's more than e-mail; it's an open platform designed for collaboration. It has proven security features and productivity enhancers like document sharing and custom app development. And it's flexible enough to integrate across multiple platforms, including J2EE™ and Linux®.
_OK, who sat on my lunch?
IBM®
Lotus®
Download the Lotus Notes & Domino demo at:
IBM.COM/**TAKEBACKCONTROL**/COLLABORATION
IBM, the IBM logo, Lotus, Notes and Domino are registered trademarks or trademarks of International Business Machines Corporation in the United States, other countries or both. Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both. Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both. ©Copyright IBM Corporation 2006. All rights reserved.

Blake Eno (products@windowsitpro.com) is product editor for *Windows IT Pro* and *SQL Server Magazine.*

RecordTS terminal services

Archive RDP Traffic for Future Playback

TSFactory helps confirm that your Windows network is secure and compliant with the release of RecordTS, an RDP-recording solution that tracks the actions users take when connected to a Windows server with Terminal Services or RDP enabled. Tracked information includes which users connect to a Terminal Server, what actions they take while connected, and the duration of their connection. RecordTS can record user activity at specific times of the day, monitor access to sensitive information such as financial records, and save server access and time/date data to digitally signed files for storage or secure playback. The software also records administrator activity on domain controllers (DCs) and Microsoft Exchange Server machines.

www.tsfactory.com,
919-677-8091, 866-344-6267

EMULEX

Optimize SAN Connectivity for Microsoft Virtual Server

Emulex released VMPilot, which provides a virtualized host bus adapter (HBA) connection for Microsoft Virtual Server 2005 environments to simplify the creation and migration of SAN-based virtual machines (VMs). The SAN connectivity virtualizes a connection to SAN-attached storage, which saves time and costs because you can migrate VMs without reconfiguring storage or copying files. VMPilot's wizard creates VMs with SAN connectivity according to industry-standard N-Port ID Virtualization and deploys and migrates SAN-based VMs while leveraging your existing SAN management tools and best practices, such as fabric zoning at the VM level.

www.emulex.com,
714-662-5600, 800-368-5391

Reduce Help Desk Calls and Increase User Productivity

www.netpro.com, 602-346-3600, 800-998-5090

NetPro Computing announced SelfServiceADmin, an addition to the company's Active Directory Administration Suite that lets end users reset their password and unlock their account without violating data-security standards. The software's Web-based portal audits and tracks end-user activity and delivers notification of successful or unsuccessful password reset results. The portal also gives admins secure access to user configuration settings across multiple domains and is available to users or administrators any time of the day. You can purchase SelfServiceADmin as a single solution or as part of NetPro's Active Directory Administration Suite.

Product Spotlight

Provision and Maintain Extranet SharePoint Sites

www.sharepointsolutions.com,
615-515-0210

SharePoint Solutions announced Extranet Collaboration Manager (ExCM) for SharePoint 2007, add-on software for Windows SharePoint Services and Microsoft SharePoint Portal Server. The software helps you collaborate effectively by providing your partners, customers, and suppliers with access to sensitive information and maintaining security, audit ability, and accountability. "SharePoint has become the leading tool for intranet collaboration," said SharePoint Solutions Founder and President Jeff Cate in a recent briefing. "But more and more IT professionals are being asked to open up their SharePoint sites to enable collaboration with people and partners outside the company firewall." Creating and maintaining these sites can greatly increase an IT department's workload. According to Cate, ExCM leverages new capabilities in SharePoint 2007 to provide provisioning, security, and monitoring functionality to extranet sites to help reduce this burden.

ExCM takes advantage of SharePoint 2007's form-based authentication and provides a wide range of options for storing extranet user data separately from your internal user accounts. It also gives SharePoint administrators the ability to delegate user management of an extranet site to a member of the external organization. Giving external business partners the ability to manage their own user accounts can significantly reduce headaches for the internal IT staff. The standard version of ExCM sells for $995; the enterprise version sells for $2995 per Web front-end server.


_INFRASTRUCTURE LOG
_DAY 33: Our information is siloed. Unmanageable. People can't access the latest info to make decisions. Gil's resorted to giving everyone access to everything all at once.
_Monitors now outnumber humans 18 to 1.
_DAY 36: It's clear to me. We need an IBM Information On Demand middleware solution. Info will be liberated from the silos—available when we need it, whatever the format. Accurate and in context. Now we can make smarter decisions and deliver real business value.
_Access is a beautiful thing.
IBM
Information Management
See innovative IBM Info Management solutions in action:
IBM.COM/TAKEBACKCONTROL/INFO
IBM and the IBM logo are registered trademarks of International Business Machines Corporation in the United States and/or other countries. ©2006 IBM Corporation. All rights reserved.

EDITOR'S NOTE: Send new product announcements to products@windowsitpro.com.

ExclamationSOFT

Continuously Monitor Your Web Site Applications and Network Infrastructure

ExclamationSoft announced WebWatchBot 5.0, software that monitors Web-based applications from an end-user perspective and also monitors network infrastructure components such as routers, servers, databases, and processes. WebWatchBot monitors Windows performance counters on local and nonlocal Windows systems, including counters for CPU and memory usage, SQL Server, Microsoft IIS, physical disks, and processes and services on most devices. The software also monitors IP addresses or host names by looking for an excessive number of hops or timeouts. The software includes SNMP-enabled monitoring, which allows monitoring of hardware and software regardless of OS. Pricing for WebWatchBot starts at $1249.95.

www.exclamationsoft.com, 267-895-1726, 866-489-0111

Protect the Integrity of Your Network Infrastructure

SmoothWall announced updates to its network security solution, Advanced Firewall 2.0. The software is a firewall and VPN system that can automatically fail over to a standby Advanced Firewall system in the event of a hardware problem. Improved load-balancing features allow a network's outgoing and incoming traffic to be load balanced across multiple Internet connections. Advanced Firewall also includes VoIP gateway protection and improved antispyware, antivirus, and browser-exploit detection capabilities. The software integrates the Mailshell spam detection engine, which blocks spam email, and new authentication supports two-factor tokens and ISP authentication.

www.smoothwall.net, 800-959-3760

GFI EventsManager

Ensure Optimum Network Utilization

GFI Software announced GFI EventsManager, a centralized networkwide event-log management and reporting solution that ensures maximum network uptime. GFI EventsManager scans and collects information from Windows event logs, World Wide Web Consortium (W3C) logs, and syslog events and translates cryptic events. Captured events are stored in a SQL Server database that can be offsite, and you can schedule backups of your event logs. The software also alerts you to potential hardware failure, detects intruders and security breaches, and proactively monitors servers. For pricing information, contact GFI Software.

www.gfi.com, 919-379-3397, 888-243-4329

NetApp Adds Fibre Channel and Replication Support to Its SMB Storage Solution

Network Appliance announced updates to its all-in-one network storage appliance solution, StoreVault S500, which provides NAS, SAN, and DAS out of the box. StoreVault S500's StoreVault Replication software copies file and block data over a WAN between multiple StoreVault S500 appliances by using the StoreVault Manager 2.0 interface. StoreVault Replication replicates only changed data, which reduces network bandwidth requirements. The software also provides replication checkpoints to reduce data loss in case a data transfer is interrupted. NetApp also announced the StoreVault Fibre Channel Starter Kit, which includes a factory-installed host bus adapter (HBA), a ten-port 4GB Fibre Channel switch, and QLogic SANsurfer Express software.

www.storevault.com, 877-278-7858

InstantDoc ID 94594

IBM
_INFRASTRUCTURE LOG
_DAY 34: This indecision is sinking the business. How do we move to a service oriented architecture? Where do we start? Can we reuse what we have?
_Infrastructure quicksand!! We waited too long. I'd throw Gil my tie, but it's a clip-on.
_DAY 37: A lifeline: IBM WebSphere middleware! It's already helped thousands of customers build an SOA. Adapters give us a standardized approach to integrating apps from SAP, Oracle and others. And it lets us reuse what we have, saving time and money.
_Oh, great. There's sand in my yogurt.
WebSphere.
Download the reuse and connectivity kit at:
IBM.COM/**TAKEBACKCONTROL**/CONNECT
IBM, the IBM logo and WebSphere are registered trademarks of International Business Machines Corporation in the United States and/or other countries. © 2006 IBM Corporation. SAP is a registered trademark of SAP AG in Germany and in several other countries. Oracle is a registered trademark of Oracle Corporation and/or its affiliates. All rights reserved.

Insights from the industry

Mitigate IPv6's Fright Factor

Today everyone is competing for IP addresses. Rather than jump into the complex realm of IPv6, many companies are scrambling to maximize their IPv4 allocations—an increasingly challenging prospect as IP addresses become scarce. (Some analysts predict that, by around 2010, we'll run out of IPv4 addresses.) IPv4 supports 4.3 billion addresses, which can't hope to fully support the exploding mobile-device market. By contrast, IPv6 supports 50 octillion addresses. That number would provide an IP address to just about every atom on Earth.

However despite its greater capacity, "IPv6 scares everyone!" said David Berg, director of product management at **BlueCat Networks** (http://www.bluecatnetworks.com). "It's *incredibly* complex." The solution is IP Address Management (IPAM), which promises to become the new industry standard in IPv6 management. BlueCat Networks is at the leading edge of this technology, developing end-to-end IPAM solutions that overcome legacy limitations—such as laboriously tracking addresses in spreadsheets or homegrown databases—and let midsized to large enterprises get the most out of their IP infrastructure.

—**Jason Bovberg**

US Companies Ready for Preboot Security Solution

Secuware (http://www.secuware.com/en) sees opportunity for its Secuware Security Framework in the United States. The Spanish company recently opened an office in Silicon Valley in response to requests by large US customers such as Wal-Mart, said Feliciano Rivera, who will head up the US operation.

Carlos Jimenez started Secuware in 1988 after selling his antivirus software company to McAfee and deciding that he wanted to create a better solution for keeping enterprises secure. The result, Secuware Security Framework, comprises a module that authenticates the user *before* Windows boots, encrypts the user's computer, and features modules for device and application control and security event auditing.

Secuware already has large customers in Spain's Ministry of Defense as well as in other European countries and in the North Atlantic Treaty Organization (NATO). Jimenez and Rivera believe that large enterprises in the United States—and smaller businesses that handle sensitive information, such as healthcare providers—are also ready for Secuware's comprehensive security infrastructure.

—**Renee Munshi**

Can You Recover Critical Data in Seconds?

I recently spoke with **Symantec Corporation** (http://www.symantec.com/index.htm) about what the company calls its biggest feature release ever, Backup Exec 11d. Frank Mong, senior director of product marketing, and Brian Greene, director of product management, told me that Backup Exec 11d's development has been driven by its customers. Symantec's customers, like everyone else, need to shrink backup windows and reduce storage media costs. But an even greater need exists for backup and recovery customers: Businesses want to protect their data on and off site but, even more important, want granular recovery in their applications—that is, recovery of critical data within seconds.

With Backup Exec 11d, administrators can recover individual Microsoft Exchange Server messages, folders, and mailboxes; Microsoft Office SharePoint Server 2007 documents; Active Directory (AD) users and properties; and SQL Server 2005 snapshots. And if you want secure backup data, Symantec offers both 128-bit and 256-bit Advanced Encryption Standard (AES) encryption.

—**Blake Eno**

InstantDoc ID 94553

High Availability Keeps RIM BlackBerry Users Connected

Executives were the first—and sometimes the only—employees —to have a BlackBerry. Now, it often seems that all employees have one. Neil Robertson, **Neverfail Group**'s (http://www.neverfailgroup.com) CEO, told me during a recent industry briefing that, by functioning as a mobile PC, the BlackBerry has transitioned from an email tool to a complete business tool that is capable of running software applications under an OS. Because of this added functionality, employees now expect to be able to reach their corporate network at any time, prompting what Robertson sees as an "interesting proliferation of applications to the [BlackBerry] tool."

Neverfail recognized that, in many businesses, productivity has become dependent on an employee being able to access the network from his or her mobile device at all times. So the company created a high-availability product: Neverfail for RIM BlackBerry. If a company's primary server goes down, Neverfail for RIM BlackBerry seamlessly switches users' workloads to a backup server so that mobile connectivity remains unbroken and productivity is not affected. When IT brings the network back online, the solution instantly switches users back to the original, primary server.

According to Robertson, Neverfail for RIM BlackBerry, and products like it, represent only the beginning of the growth of mobile device applications and their impact on business. "Currently, screen size is the only limiting factor; in two years all mobile devices will have the ability to do everything a PC can do," said Robertson.

—**Megan Bearly**


IBM
_INFRASTRUCTURE LOG
_DAY 27: These compliance regulations are killing us! Audits. Inconsistencies. Processes. Time. Money. I feel like I'm being chased by regulators.
_Oh, wait. I am being chased by regulators. Run!!!!!
_DAY 28: I've got it: IBM Tivoli middleware. It automates system administration to standardize compliance policies. It centralizes processes to minimize the headaches of new and ever-changing regulations. And it helps pinpoint security issues before they become problems and maintains business integrity.
_Gil is bummed we had to ditch the high-carb diet.
Tivoli.
Better manage the business of I.T. at:
IBM.COM/**TAKEBACKCONTROL**/COMPLIANCE


NO
Refund
Exchange
ONLY

Disk Imaging Software for SMBs

3 popular tools aid desktop deployment and backup

by Joel B. Barker

One of my first IT jobs was working on a 2000-seat desktop migration to Windows 2000. Our team faced a daunting set of challenges: preserving locally stored data, managing the array of drivers required to keep a diverse installed base humming, efficiently deploying managed desktops across a campus. We dubbed our eventual solution "the octopus cart." It was a four-wheeled cart with a server running Symantec Ghost, a switch, and a bag of patch cords. We rolled our cart into an office and idled a dozen workers for two to three hours while we ran a custom backup script, deployed the new OS, restored data, and then dealt with BIOS and driver issues.

With more robust networks and more cooperative hardware and OSs, organizations today prefer desktop deployment over the network to the in-person utility-cart method. Imaging software is at the core of these strategies. I tested three popular tools to find viable imaging solutions for desktop deployment and backup for a small or midsized business (SMB). **Symantec** Ghost Solution Suite offers systems management features in addition to imaging. The other two products I reviewed—**Acronis** True Image Workstation and **Paragon Software**'s Paragon Drive Backup Professional focus more narrowly on imaging for backup and deployment.

Key Features

Imaging at its most basic is bundling an entire drive or partition as a file and then restoring it to another partition or drive. Imaging products can serve a business of any size as a long-term investment. Distributed organizations can benefit from centrally controlled imaging that a system administrator can deliver and track from one location.

I used three criteria to evaluate Symantec Ghost Solution Suite, Acronis True Image Workstation, and Paragon Drive Backup Professional. First, I looked at how well each application backs up and recovers individual files or complete disks. Second, I tested how the product performs desktop deployment. You can use any desktop imaging tool to make an exact copy of a hard drive and restore it on other identical machines, but more sophisticated tools can also automate the Microsoft Sysprep utility and driver injection to deploy and manage an OS on varying hardware platforms. Third, I examined the performance of the three imaging products. I used each application to do an identical imaging and restoration job across a network to compare the applications' speed.

Symantec Ghost Solution Suite

The venerable Ghost, purchased by Symantec in 1998, has gone through several iterations over the years. The most recent version, Symantec Ghost Solution Suite, bundles imaging and deployment with some desktop systems management capabilities. Version 1.1 of the suite, which I tested, includes Symantec Ghost 8.3, Symantec Deploy Center 5.6.1, and Symantec Client Migration 3.0.2. In addition to imaging and deployment, Ghost Solution Suite can track the installed base, inventory installed hardware and software, and install new software packages remotely. Think of Ghost Solution Suite as a competitor to Microsoft Systems Management Server (SMS) with a focus on desktop deployment.

Organizations today prefer desktop deployment over the network to the in-person utility-cart method

Ghost Solution Suite has an elegant backup and recovery feature. Differential backups can be regularly scheduled and triggered remotely for managed computers, including groups of computers. Each backup or recovery requires the client computer to boot to the Ghost environment, idling anyone who might have been trying to use the computer at the time. The other two imaging products in this review cleverly utilize Microsoft Volume Shadow Copy Service (VSS) to create the image without interfering with current operations.

Although Ghost Solution Suite is capable of creating images of Linux machines, it's clearly geared toward Windows, with many Windows- and Active Directory (AD)-specific integration points. For instance, Ghost can migrate a Windows user's data and state. Ghost Solution Suite retains the features that made Ghost the gold standard for imaging, all controlled via a central console. For example, tasks such as deployments can be scheduled.

One particularly useful tool for deployment is Ghost's multicast feature. When you initiate a larger scale image deployment, multiple clients can download a single image transmitted from the console, significantly cutting down on the bandwidth required for remote deployment. Midsized

Summary

EDITORS' CHOICE WindowsITPro

Symantec Ghost Solution Suite

PROS: Automated deployment features; multicasting and throughput limitation features, some systems management features, reasonable price

CONS: Backup and restore processes take over machine, idling users; extra features mean added complexity for small IT staffs

RATING: ◆◆◆◆◇

PRICE: $39.20 per seat with volume discounts

RECOMMENDATION: The Editor's Choice product and not just for imaging anymore, Ghost Solution Suite is a management and deployment tool that approaches the capabilities of SMS for less than half the price.

CONTACT: Symantec • 800-441-7234 • http://www.symantec.com

and large companies can benefit from multicasting to reduce the impact of deployment on the network. In addition, Ghost can limit throughput so that a deployment won't saturate the network.

Creating a 4GB image over a network connection took 30 minutes. Restoring the same image to the same workstation took 20 minutes.

A new feature in Ghost Solution Suite is the ability to edit existing images as files. Thus you can make configuration changes or add upgraded applications to an image without creating an entirely new base image.

For midsized and large companies, Symantec offers a panoply of features at an inviting price. These include the ability to inventory the enterprise's software and hardware and deploy software. Considering the array of features, the interface (which Figure 1 shows) is quite clean. However, I'd prefer to see more wizards and fewer tabbed dialog boxes. Ghost Solution Suite has a more gentle learning curve than that of the desktop management powerhouse Microsoft SMS and is significantly easier to set up. However, Ghost does require some significant energy from the IT team to realize the product's benefits. It's my selection for Editor's Choice, although it has more features than what a small business would typically want or need.

Acronis True Image Workstation with Acronis Universal Restore

Acronis True Image Workstation is designed primarily for easy backup and recovery. Images can be differentially backed up, and differential backups can be scheduled and triggered remotely. I tested True Image 9.1.

True Image's interface (which Figure 2 shows) is intuitive, well explained, and easy to use. Just minutes after I installed each element of True Image (the local application, the workstation tools, and the administrative tools), I was able to create a new backup and schedule a backup task. True Image would be a good tool to use to implement an ongoing service level agreement (SLA)-based backup and recovery strategy.

One major advantage of True Image is that you can create backups from within the OS while other applications run. By using VSS, True Image can create a complete disk image backup while applications are running and files are open. As a result, scheduling backups isn't as difficult. Of course, restoring a disk does require booting to a preinstallation environment.

In my test, creating a 4GB image over a network connection took 8 minutes. Restoring the same image to the same workstation took 12 minutes. This is much faster performance than Ghost, on an individual machine. However, Ghost's multicast feature would give Ghost the performance edge in a larger deployment.

Although not specifically targeted toward deployment, True Image includes some features and add-ons that make it useable for small deployments or desktop refreshes. When you design an image restore, you can define pre- and post-installation tasks for True Image to perform, such as initiating Microsoft Windows User State Migration Toolkit (USMT) and Sysprep. With these scripted tasks and Acronis Universal Restore (described below), an administrator could refresh a desktop or migrate a client with True Image.

Because True Image simply copies an image of a partition or drive, it's not on its own

Summary

Acronis True Image Workstation with Acronis Universal Restore

PROS: Can create image without booting to preinstallation environment; fast backup and restore

CONS: Some scripting plus Microsoft's USMT and Sysprep are required for automated deployment; high price

RATING: ◆◆◆◇◇

PRICE: True Image: $79.99 per seat with volume discounts; Universal Restore: $29.99 per seat with volume discounts

RECOMMENDATION: This product is easy to deploy and use and is a great desktop backup and recovery solution for SMBs that can afford it. True Image has rudimentary but effective tools for performing small-scale deployments but isn't an enterprise-level deployment solution.

CONTACT: Acronis • 877-669-9749 • http://www.acronis.com

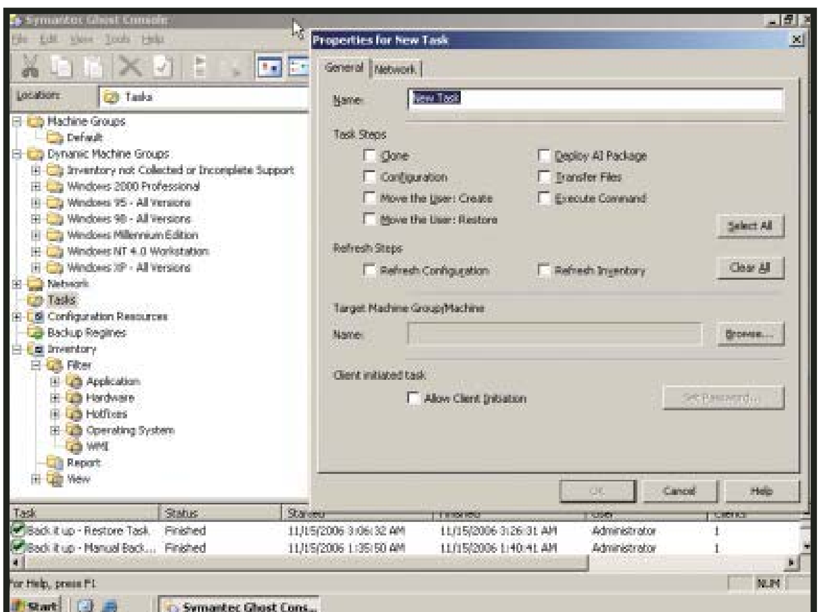


Figure 1: Symantec Ghost console

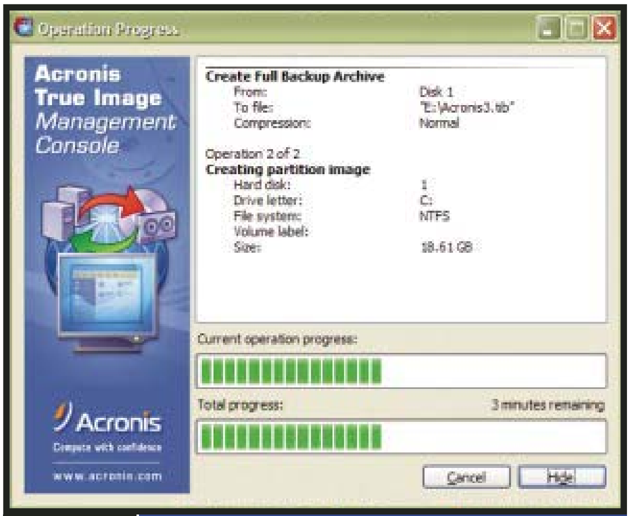


Figure 2: Acronis True Image management console

suited to large-scale deployments. However, the add-on product Acronis Universal Restore allows driver injection and preserves the current SID of the target computer. Universal Restore can restore an image to a replacement computer even if the replacement doesn't have the same hardware as the failed machine.

True Image includes a feature called Secure Zone, which lets you create a recovery partition on a workstation and automatically schedule backups to that location. Users can recover individual files or restore an entire drive from this partition without the assistance of IT personnel and without access to the network. Of course, this is only a partial recovery solution—it wouldn't be of help in instances where the entire disk is damaged or inaccessible.

True Image does have an administrative remote control that you can use to connect to a remote workstation and perform all the tasks that you can perform locally. Using this management tool, you can launch group jobs or manage individual clients running the True Image agent. However, this isn't a tool that a large organization could rely upon—the remote console isn't capable of controlling groups.

Acronis True Image is easy to use and can be quickly deployed. Its backup features would definitely come in handy in a small organization in which its relatively high price isn't a problem. However, it's not an ideal image deployment tool for a 10,000-workstation enterprise. Look to this tool for data protection and disaster recovery or, with the addition of Universal Restore, workstation imaging in a small network. Particularly advantageous is the use of VSS to allow for backups while the computer is in use.

Paragon Drive Backup Professional Edition

Paragon Drive Backup Professional Edition is intended for just that: creating an image for backing up and restoring partitions. A lot of the features of Drive Backup 8.0, the version I tested, compare with those of Acronis True Image. Like True Image, Drive Backup can back up without a reboot and while other applications are running. It can schedule backups—including differential backups—and place them on a hidden partition. It can clone an image to another identical or nearly identical drive and change the SID. It allows the user to browse an image and restore individual files from an image.

Drive Backup lacks the extra features that make Symantec Ghost and True Image worthwhile applications for IT departments. It has no remote management tools and no option for scripting USMT or Sysprep.

The user interface (which Figure 3 shows) is a simple embedded browser but still managed to be somewhat confusing. After I completed the Create an Image wizard, nothing happened. I repeated the wizard, thinking that I had missed something. Still nothing. Finally, I noticed the View Changes, Apply, and Discard buttons on the toolbar. I had to click Apply before the task would run. Given that the only functions are to create a backup, restore a backup, and copy a disk on the local workstation, it seems unnecessary and counter-productive to schedule a series of jobs and perform them. The jobs would conflict with each other.

A scheduled backup job to create a 4GB image over a network connection took well over an hour. Restoring the same image to the same workstation also took over an hour.

Summary

Paragon Drive Backup Professional Edition

PROS: Can create image without booting to preinstallation environment
CONS: No remote management tools and no option for scripting USMT or Sysprep; confusing UI; slow backup and restore
RATING: ◆◇◇◇◇
PRICE: $49.95 per seat with volume discounts
RECOMMENDATION: I can recommend this product for only very small businesses that can't handle the feature set of Symantec Ghost or the price of Acronis True Image.
CONTACT: Paragon Software • 800-240-8993 • http://www.paragon-software.com

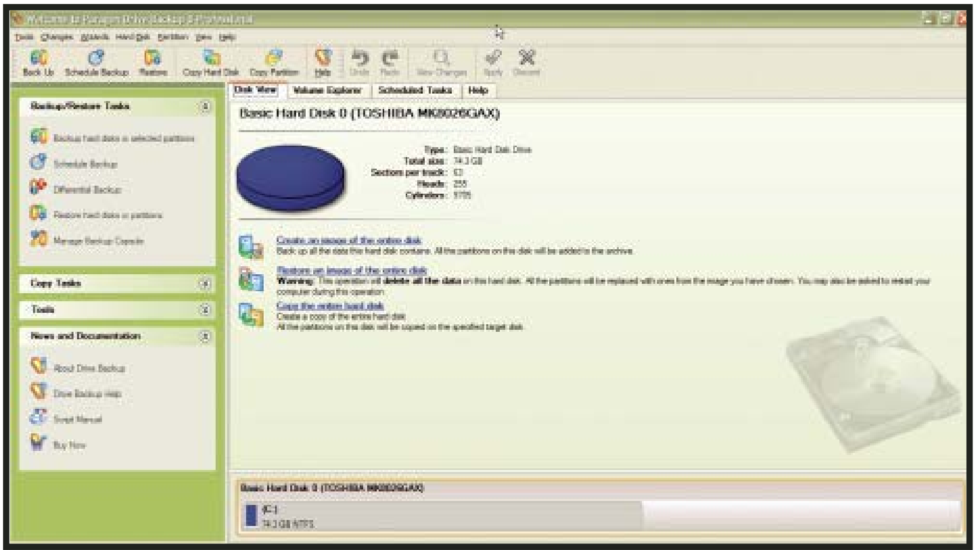


Figure 3: Paragon Drive Backup console

Drive Backup offers no features that would favor it over Acronis True Image except for price. Symantec Ghost's many features outweigh Drive Backup's ability to back up without a reboot and while other applications are running.

Vista and Microsoft

The deployment scenario that's on everyone's mind these days is deployment of the new Windows Vista desktop. Microsoft is releasing Windows Deployment Services (WDS), the latest version of Remote Installation Services (RIS). WDS uses the new Microsoft Windows Imaging Format (WIM), which is editable and can handle multiple images within one file. The WIM file format isn't useable for backups, but it will change the way that deployment is managed.

Symantec Ghost Solution Suite 2.0 wasn't yet available as of this writing, but it's supposed to be Vista compatible. Acronis True Image 10.0 Home supports Vista, but the True Image Workstation 9.1 version that I tested wasn't Vista aware. True Image's and Paragon Drive Backup's backup and restore features will function on a Vista desktop.

In addition to SMS, Microsoft has another product which, along with Vista, should be mentioned in the deployment space. Business Desktop Deployment (BDD) 2007 is currently in beta 2 testing. The previous versions of BDD, 2.0 and 2.5, were a collection of guidance and best practice documents. BDD 2007 is more of an "on the ground" tool that includes applications and wizards that package and deploy WIM files and applications, especially Microsoft Office 2007. BDD isn't a tool for backup, but SMBs looking to deploy Vista should certainly evaluate this tool for their Vista deployment—particularly at the low price of free.

The Bottom Line

Larger organizations can justify the cost of SMS and similar enterprise-class management servers, but small IT departments have generally been priced out of any kind of deployment tool beyond a technician with a custom image on a DVD. Symantec Ghost Solution Suite is an affordable product that offers a set of features similar to SMS as well as the ability to launch and manage desktop backup routines.

For organizations not interested in Ghost's feature set that need only to deploy the occasional new workstation and keep some critical laptops backed up, Acronis True Image Workstation is a sharp program. It's targeted right at an SMB's desktop backup and deployment needs. Although more expensive than Ghost, the ease of setup and deployment would be a boon to understaffed, overworked SMB IT staffs. It does exactly what it should with little effort or risk. It's appealing for its incredibly easy deployment path as well as its use of VSS to create images of a disk while the disk's OS is in use.

InstantDoc ID 94593

Joel B. Barker
(jbarker@aeshen.com) is a product reviewer for Aeshen.

Paul's Picks

Summaries of in-depth product reviews on Paul Thurrott's SuperSite for Windows

http://www.winsupersite.com

Microsoft Internet Explorer (IE) 7.0

PROS: Major functional advances, better security, printing feature is top-notch
CONS: Best security features available only on Windows Vista
RECOMMENDATIONS: Now fully on par with third-party browsers such as Mozilla Firefox, IE 7.0 includes major security advances and features such as tabbed browsing. Unfortunately, two of IE 7.0's best security features—Protected Mode and parental controls integration—require Windows Vista. Relatively small shortfalls shouldn't detract from a product that is so much safer than IE 6.0 it's almost hilarious. Anyone stuck with IE 6.0 should upgrade as soon as possible.
CONTACT: Microsoft • 800-426-9400 • http://www.microsoft.com
FULL REVIEW: http://www.winsupersite.com/reviews/ie7.asp

Microsoft Zune

PROS: Simplified UI, big screen
CONS: Online store is a joke; incompatible with iTunes and PlaysForSure-based content
RECOMMENDATIONS: Microsoft's initial Zune portable media player comes up short in a feature-by-feature comparison test with Apple's dominant iPod and even many PlaysForSure-based devices, but it's still a solid effort. The device boasts a large, colorful screen, an uncomplicated UI, and PC software that is simpler than either iTunes or Windows Media Player. But the devil is in the details: Zune users can't purchase or download TV shows or movies, and can't access much of the online media that iPod users can. Hold off on this promising but somewhat-lacking media player.
CONTACT: Microsoft • 800-426-9400 • http://www.microsoft.com
FULL REVIEW: http://www.winsupersite.com/reviews/zune.asp

InstantDoc ID 94688

Quest Site Administrator for SharePoint

With **Quest Software**'s release of Quest Site Administrator for SharePoint, administrators now have a comprehensive tool for managing multiple Microsoft SharePoint Portal Server 2003 servers and Windows SharePoint Services 2.0 across the enterprise. Quest will add support for Microsoft Office SharePoint Server 2007 and Windows SharePoint Services 3.0 in first quarter 2007.

Installing Quest Site Administrator for SharePoint was comprehensive, with compatibility checks that ensured that previously installed software applications were compatible with Site Administrator. My only concern was with the Report Server virtual directory page. The default setting points to http://myserver/reportserver. This poses no problem if the administrator chooses the default configuration during the installation of Microsoft SQL Server Reporting Services, but if another directory name is chosen, the Site Administrator installation will fail.

At the management console, which Figure 1 shows, the navigation tree contains the three main components that help you manage your SharePoint servers. They are Enterprise SharePoint, for discovery and maintenance of SharePoint servers; Report Manager, for reports about the usage and viability of these servers; and Policy Manager, for the creation and application of policies for these servers.

Site Administrator provides a consistent UI for administrators by framing all SharePoint Web administration and reporting functionality within one management console, reducing the time required to find and maintain Web sites on multiple servers. The reporting features provide a good overall view of the status of all managed servers. For the full-length version of this review, go to http://www.windowsitpro.com and enter InstantDoc ID 94601.

InstantDoc ID 94601

—Michael D. Cassens

Summary

Quest Site Administrator for SharePoint

PROS: Simplifies management of multiple SharePoint servers
CONS: Reports not customizable
RATING: ◆◆◆◆◇
PRICE: $10 per managed user
RECOMMENDATION: Useful for administrators who need to manage three or more SharePoint servers across a large-scale network.
CONTACT: Quest Software • 949-754-8000 • www.quest.com

Figure 1: Management console for Quest Site Administrator for SharePoint

Lose that important file?

Protect against accidental file deletions with NEW Undelete® 5

Now with version protection for Microsoft® Office files

According to the New York Times, file loss costs businesses an estimated $13 billion per year. The problem is that the Windows® recycle bin doesn't capture every deleted file, particularly files deleted over the network and older "saved-over" versions of Microsoft Office files. Not even your backup system provides comprehensive real-time protection.

Now you can get *complete* up-to-the-minute file protection with instant recovery—get new Undelete 5!

- **NEW!** Version protection allows *instant* recovery of older versions of Microsoft Word, Excel and PowerPoint® files
- **EXCLUSIVE!** Recovery of deleted files is easy and *instant*
- **EXCLUSIVE!** Undelete 5 captures and protects *all* deleted files in real time—even files deleted by other systems over the network. No more lengthy backup restores!
- Server and workstation editions available

Try Undelete FREE!
Visit: www.undelete.com/winUD5

For volume license pricing and government or educational discounts, contact your favorite reseller or call 800-829-6468 reference number 4330

Diskeeper corporation

HP StorageWorks 400 All-in-One Storage System

Meeting the ever-growing need for storage is a problem that all IT organizations face. Larger organizations typically opt for Fibre Channel SAN–based solutions, but these are often too costly and too complex for small-to-midsized businesses (SMBs). The **HP** StorageWorks 400 All-in-One Storage System (AiO400) is designed to fill the storage needs of SMBs. It can be used for file serving, print serving, Microsoft Exchange Server or Microsoft SQL Server storage, custom application storage, or backup and data protection. It provides iSCSI SAN support as well as integrated NAS support.

The AiO400 is a 1U rack-mounted appliance that comes preloaded with Windows Storage Server 2003 R2, Standard Edition. The unit I tested was equipped with four 250GB Serial ATA (SATA) drives, 1GB of RAM (with support for a maximum of 4GB of RAM), and a 3.0GHz dual-core Intel Pentium D processor. The unit also came with a slimline 8x DVD+RW, two front USB ports, two rear USB ports, one rear serial port, two 10/100/1000GB Network Controller Interfaces, one VGA port, and PS/2-style keyboard and mouse ports. Internally, the AiO400 can be expanded through use of either the low-profile, half-length PCI Extended (PCI-X) slot or the full-height, full-length PCI-X slot. For added disk storage, the unit

The AiO400 is a great storage solution for SMBs looking for easy-to-manage storage

can also attach to an external HP StorageWorks Modular Smart Array 20 storage device.

Getting the unit up and running was a snap. After installing the unit in the rack and plugging in the power, I connected one of the Ethernet ports to my standard LAN infrastructure; I connected the other Ethernet port to a dedicated iSCSI LAN, which helps to ensure adequate bandwidth for other iSCSI servers that utilize the AiO400. You can manage the system by using either a remote browser or the AiO400's ports for external keyboard, mouse, and monitor. I opted to use the direct-attach method.

When I turned the unit on, it went through a 10-minute installation, after which the system logon prompt was displayed. The Rapid Startup Wizard allowed me to set the date and time, administrative password, network configuration, and server name as well as alerts and SNMP information. The system then rebooted and was ready to run. A storage wizard lets you easily set up the type of storage the appliance will be used for. Storage options include creating shared folders, hosting an Exchange storage group, hosting a SQL Server database, or creating user-defined application storage. The wizard also lets you schedule data migrations from existing locations to the AiO400. Before you can schedule migrations, you must install the All-In-One Storage Manager agent from the setup CD-ROM onto the target servers. The unit's Storage Server interface in combination with the setup and storage wizards makes the unit very easy to manage.

The AiO400's file-serving capabilities include both Common Internet File System (CIFS) and NFS support. The appliance includes iSCSI initiator support for Windows, Linux, BSD, AIX, and Sun Microsystems Solaris. HP's sizing recommendation notes that the unit can support as many as 200 Exchange mailboxes. For data protection, the storage server supports as many as 256 snapshots per volume. The included HP StorageWorks Data Protector Express software enables data to be backed up and recovered from tape, virtual tape, optical storage, or external networked disk. The unit also supports setting up Distributed File System Replication (DFSR) to a second AiO400 or to the next bigger model, the HP StorageWorks 600 All-in-One Storage System.

The AiO400 is a great storage solution for SMBs looking for easy-to-manage storage with a reasonable price tag. Its iSCSI options don't require specialized and expensive Fibre Channel equipment. The appliance's setup is simple, and the included setup and storage wizards bring the task of configuration within the reach of the heavily burdened SMB administrator.

—**Michael Otey**

InstantDoc ID 94535

Summary

HP StorageWorks 400 All-in-One Storage System

PROS: 1U size takes minimal rack space; easy to set up and manage; well constructed and quiet

CONS: The low-end 400 unit doesn't include redundant power supplies and fans

RATING: ◆◆◆◆◇

PRICE: Starts at $5499; tested configuration, $5499

RECOMMENDATION: The HP StorageWorks 400 All-in-One Storage System is a great choice for SMBs looking for an iSCSI storage solution.

CONTACT: HP • 800-752-0900 • http://www.hp.com

Get the answers you need to 3 big file-and-print problems

FILE AND PRINT ANNOYANCES

BY JOHN SAVILL

I hear about certain file and print "challenges" over and over again from clients. Visitors of my Web site echo these annoyances. I want to address three of the most popular complaints I hear on this subject: the inability to restrict file shares, to deploy printers via Group Policy, and to control quota usage.

Too often, we give in to the temptation of reaching out to third-party solutions rather than using freely available, built-in OS tools. In particular, Windows Server 2003 Release 2 (R2) and the forthcoming Longhorn Server offer terrific file and print management solutions.

Can't Restrict File Shares

File services have vastly matured in Windows, but there are always features that other network OSs have that Windows doesn't (or hasn't had before now). One such feature is visibility of folders and files to which users don't have permissions. In OSs such as Novell NetWare, users see only the files and folders to which they have access, whereas in Windows, users typically see all shared files and folders—even those to which they're denied access. Perhaps this default behavior doesn't seem significant, but users can often glean an idea of file contents from filenames. For example, the file *John Savill reasons to fire.doc* would make me uncomfortable even though I can't see what's in the file. And depending on industry type, this hint of data content might break regulations and compliance requirements.

To solve this problem, Microsoft has released Windows Server 2003 Access-based Enumeration, a downloadable add-on for Windows 2003 Service Pack 1 (SP1) that you can obtain from Microsoft's Web site. This tool lets you control—at the server or individual share level—the ability for users to see only the files and folders to which they have access. Downloads are available for both 32-bit and 64-bit versions of the OS; although Windows 2003 SP1 is discussed, Windows 2003 R2 is also fully supported (since Windows 2003 R2 is essentially Windows 2003 SP1 with "extras").

The installation procedure prompts you to enable access-based enumeration for all folders or to allow folders to be individually enabled (the default option). After installation, the properties of a shared folder will have a new tab—*Access-based Enumeration*—which Figure 1 shows. On this tab, you configure folders so that only users who have at least Read permissions can view them.

A command-line tool called Abecmd is also provided as part of the download. This tool gives you command-line control of access-based enumeration.

Can't Deploy Printers via Group Policy

Longhorn Server will offer full support for printer deployment and management, but until we're all enjoying Longhorn Server and Windows Vista clients, most of us are turning to third-party alternatives for help in the management of printer deployments. However, you might not know about an interim solution that's part of Windows 2003 R2—a feature that helps fill the gap between what we have today in terms of printer deployment via Group Policy (i.e., zero functionality) and Longhorn (i.e., a useful set of tools). The new Print Management Console aids in the management of print servers both locally and remotely, and it lets you push printers via Group Policy.

There is a caveat. Typically, the client reads and automatically processes Group Policy settings; obviously, legacy clients won't understand the Windows 2003 R2 print-deployment capabilities of Group Policy. Therefore, you'll need to install a client-side piece on those computers so that you can process printers they should connect to. These client pieces are usually Client Side Extensions (CSEs), which are part of the OS and executed automatically as required to process Group Policy settings. For example, there are Folder Redirection, Administrative Template, and Security

CSEs—to name a few. Unfortunately, there's no Printer Connections CSE in Windows XP. (Vista will have one.) So, in addition to setting Group Policy options for the actual printers, you'll need to deploy a command-line utility—Pushprinterconnections.exe—to run at machine startup or user logon (accomplished through a startup or logon script).

To install the Print Management Console, open the Control Panel Add/Remove Programs applet and find the tool in Add/Remove Windows Components. During installation, the system creates a folder called PMCSnap under the Windows folder. The PMCSnap folder contains the files that the Print Management Console will use, including the new Microsoft Management Console (MMC) Print Management snap-in and the client-side Pushprinterconnections.exe image.

A word of caution: The Pushprinterconnections.exe tool automatically matches the processor type of the server on which you enable it. For example, if I'm running on 64-bit Windows 2003 R2, the Pushprinterconnections.exe tool installed on the server will be the 64-bit version, which won't run on most client platforms. Therefore, you'll need to take Pushprinterconnections.exe from the 32-bit Windows 2003 R2 CD (the second disc), and you'll need to manually expand it by using the Expand command on the \CMPNENTS\R2\PUSHPRINTERCONNECTIONS.EX_ file.

After you've installed the Print Management Console, you can deploy printers through Group Policy as follows:

1. Open the Print Management MMC snap-in by clicking Start, Programs, Administrative Tools, Print Management.

2. Expand the Print Servers branch, click the print server that hosts the printer, and select Printers.

3. Right-click the printer that you want to use Group Policy to deploy, and select *Deploy with Group Policy.*

4. To find the GPO name to use, click Browse.

5. Click the New GPO icon (or select an existing GPO), use the name Deploy Printers, and click OK. You need to ensure that this Group Policy is applied to a container that holds the users and computers to which you want to install this printer.

6. Select either *The users that this GPO applies to (per user)* or *The computers that this GPO applies to (per machine)*, or both, and click Add, as Figure 2, page 28, shows.

7. Click OK.

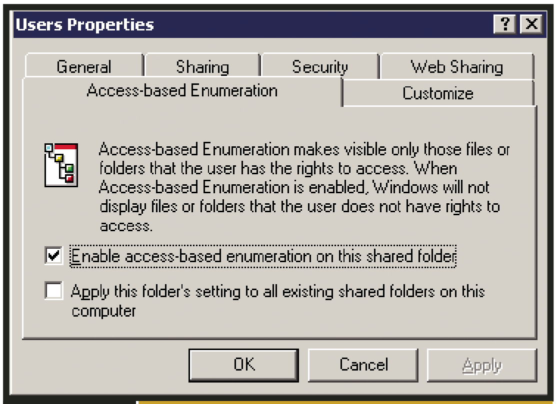


Figure 1: Enabling access-based enumeration on a per-folder basis

IT Pro Hero

DNS-AD Rescue

BY ERIC B. RUX

How I bailed a colleague out of DNS-AD chaos resulting from an ill-conceived upgrade

When I was in high school, I received my scuba certification. The most valuable lesson in that class: Stop, think, and do a little planning before you jump into the water. Failure to heed this warning could cause the bends, or possibly death. Our instructor's mantra: Plan your dive; dive your plan.

The same philosophy applies to network administrators performing large upgrades or implementing a new technology that could affect production. Too often I've seen otherwise competent technologists paint themselves into a corner because they lack a clearly defined implementation roadmap. Instead, they simply pop in the upgrade CD-ROM, double-click setup.exe, and walk through the wizard. This approach almost always leads to disaster.

This happened recently to an administrator acquaintance of mine who was trying to upgrade his Windows NT 4.0 domain to Active Directory (AD) and Windows Server 2003. He was new to network administration and didn't realize the importance of having a well-thought-out plan. Eventually, he asked for help, but by then host names weren't resolving correctly, Group Policy didn't work, and the event logs were full of errors.

We talked through the issues on an online forum, via email, and eventually over the phone. From what he described, it appeared that DNS and AD weren't communicating with each other. Here I'll talk about what we did to fix the problem (during a weekend, mind you), and in the Web-exclusive sidebar "Plan Your Dive, Dive Your Plan," http://www.windowsitpro.com, InstantDoc ID 94735, I explain my tried-and-true approach to planning that helps me avoid the kinds of snafus that befell my administrator friend.

If you open the Group Policy Object (GPO), you'll notice a new Deployed Printers branch that lists deployed printers in the GPO.

You now need to assign Pushprinterconnections.exe so that the selected printers are processed when the computer starts or when users log on (depending on the target for the printer deployment—user or computer).

1. In the GPO Editor, open the GPO that you used for the printer deployment.

2. If the selected printer is deployed to users, navigate to User Configuration, Windows Settings, Scripts (Logon/Logoff). If the printer is deployed to computers, navigate to Computer Configuration, Windows Settings, Scripts (Startup/Shutdown).

3. Right-click Startup or Logon, then click Properties.

4. In the Logon Properties or Startup Properties dialog box, click Show Files. In the Address field, you'll see the location of the scripts—for example, \\savilltech.com\SysVol\savilltech.com\Policies\{EAB0039E-A677-4C89-9CF2-053576CDA1FC}\Machine\Scripts\Startup.

5. Copy the Pushprinterconnections.exe file from the C:\windows\PMCSnap folder (or, if you're using a 64-bit server, copy the 32-bit version from the 32-bit CD) to this location, then close the window.

6. In the Logon Properties or Startup Properties dialog box, click Add.

7. Type *pushprinterconnections.exe* in the Script Name field. (If you want to enable logging, type *-log* in the Script Parameters field on the computer to which the policy is applied. For per-computer connections, log files are written to %windir%\Temp\PpcMachine.log; for per-user connections, log files are written to %temp%\PpcUser.log.)

8. Click OK.

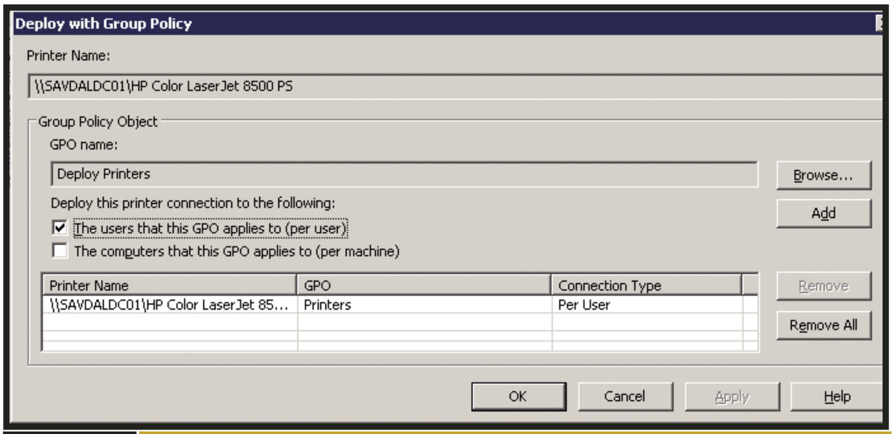


Figure 2: Deploying printers through Group Policy

For per-user deployed printers, you should now log off, then log back on. For per-machine deployed printers, you should restart the targeted computer.

The use of Pushprinterconnections.exe—while not ideal—isn't a major deployment consideration. Also, the generated log files give you information that you can use for debugging should the deployment not work. You can also look on the machines that are targets for deployment by checking the HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\PPC or HKEY_CURRENT_USER\SOFTWARE\Microsoft\PPC registry subkey, whose default value is a multivalue string, each line of which is a printer that needs to be connected through Pushprinterconnections.exe.

Can't Control Quota Usage

Quotas can be extremely useful. However, users sometimes have a tendency to misuse the space. Quota reports can tell you how users are utilizing that space, but it can be difficult to prevent users from writing illegal file types in the first place.

One of the huge wins for Windows 2003 R2 is the File Server Resource Management (FSRM)

IT Pro Hero

AD-DNS Chaos

We found these AD and DNS problems (among other, less severe ones):

- Domain controllers (DCs) didn't point to a DNS server.
- AD DNS Resource Records (RRs)—_msdcs, _sites, _tcp , and _udp—were missing.
- DNS wasn't set to accept dynamic updates.
- Clients pointed to the ISP's DNS server instead of an internal DNS server.

The administrator didn't understand the importance of DNS in an AD environment. No DNS means no AD. Finding that the AD DNS entries were blank provided me a great opportunity to explain to the admin the importance of DNS and how it worked. After we configured the correct DNS settings on each DC, we moved on to dealing with the next problem: the missing RRs.

When I looked in the DNS zone for the domain, it immediately didn't look right. I couldn't place my finger on the problem at first until I went back to my test domain and compared mine with the administrator's. Then the problem stuck out like a sore thumb: His domain didn't have the needed RRs! This adventure was getting more exciting by the minute. I had him reboot the DC, fully expecting the missing information to reappear. But rebooting didn't restore the absent RRs, so my next step was to have the admin cycle the Netlogon service by entering the following at the command line:

```
net stop netlogon
net start netlogon
```

Still no RRs. Eventually, we turned to Microsoft Help and Support and found the article "How to reinstall a dynamic DNS Active Directory-integrated zone" (http://support.microsoft.com/?kbid=294328). We

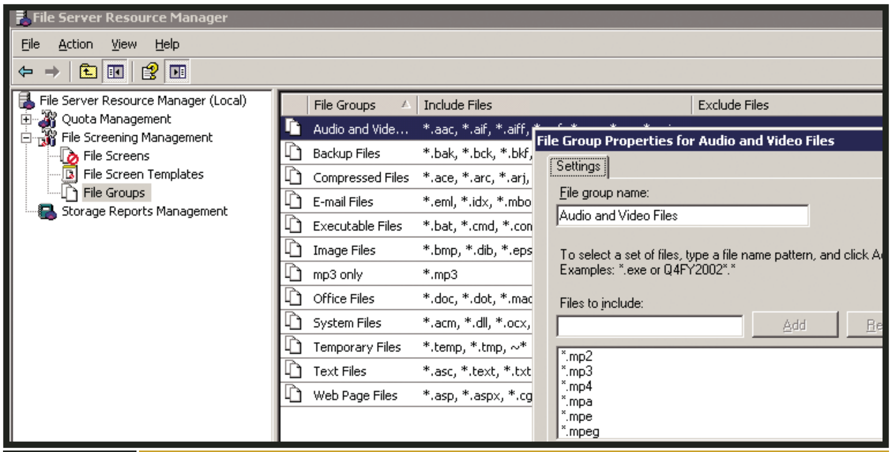


Figure 3: The MMC File Server Resource Manager snap-in

component. In addition to its powerful reporting capabilities and a new quota system that accounts for the disk's physical size (as opposed to the logical size) with disk-level and folder-level targeted quotas, FSRM includes a real-time engine that enables file-type enforcement based on file extensions. This new screening technology checks a file's extension—for example, if it's an MP3 file, the system knows it's a music file, and therefore a policy to stop music files can act on the file. If a user renames a music file to music.not_a_mp3, the system wouldn't detect the file. The system doesn't check the file's contents. However, the purpose of the technology is to stop the "accidental" offender.

You manage file screening through the MMC File Server Resource Manager snap-in, which Figure 3 shows. The default installation contains a number of file-group types, which are definitions of common file extensions and their content. For example, there's an *Audio and Video Files* group that contains nearly all known extensions. Once file groups exist, you can apply a file screen to a disk or folder to enforce certain behavior toward one or more file groups.

You can create an active or passive file screen. If a certain file is a banned file type, an active file screen actually stops the file—in real time—from being written; a passive screen allows the writing of the file but will perform a particular action that you've defined. For a given file screen, you can define a comprehensive set of actions to be performed in the event of an offense (i.e., file activity of a screened file type). These actions include sending an email message to the user or administrator, creating an event log, and creating a report that shows how a certain user is using disk space. You can also initiate a custom action.

The first action type—sending an email message—is crucial to the success of a file-screen rollout. Remember that file screening is a new server-side technology; file screens are invisible to client OSs, and if a user attempted to write a screened file type, he or she would simply receive an *Access denied* message, then probably get on the phone to the Help desk. By configuring an email action to occur seconds after the *Access denied* message, you can inform the user, with your own custom text, that company policy prohibits the type of file he or she was attempting to write and that the user should refer to a URL for a full list of company policies surrounding file server usage. Microsoft supplies 11 standard File Groups, which you can modify to add additional file types as necessary.

To avoid the need to recreate actions every time you set a file screen, you can define the actions on templates. You can apply a template to a specific file group, then apply it to disks and folders as necessary. To create a file screen, follow these steps:

1. Open the MMC File System Resource Manager snap-in by clicking Start, Programs, Administrative Tools, File Server Resource Manager.

2. Expand the File Screening Management

IT Pro Hero

followed the steps in that article to totally remove DNS and reinstall it fresh. The process was straightforward and fixed the problem.

More DNS Troubles

The third issue we discovered—that DNS wasn't set to accept dynamic updates—could also explain why some of the PCs weren't resolving IP addresses correctly. The PCs had entries in DNS, yet those entries weren't being updated when the PCs' IP addresses changed via DHCP. The solution was simply to configure the clients to allow DNS dynamic updates.

The last problem we found is something that I see a lot when companies migrate from NT to AD. In NT, there usually wasn't a reason to use DNS to resolve host names; we just used WINS to resolve NetBIOS names. DNS then was left to resolve Internet names for browsing in Internet explorer (IE). This process worked well in an NT environment, but it's a paradigm that needs to change when you move to AD. Client computers need their DNS to point to an internal DNS server so that AD services such as Group Policy work correctly. In Windows 200x, you live and die by DNS.

Situation Normal

It took a few days for us to straighten out all the glitches in the administrator's network, but in the end the network was spinning like a top. Although you can't foresee every network trouble that could occur when you perform a major OS upgrade, in my experience I've learned that having a carefully considered upgrade plan in place—and following that plan—go a long way toward avoiding the type of snafus that plagued my network administrator colleague.

InstantDoc ID 94736

Eric B. Rux

(ebrux@mvps.org) is a senior Windows administrator for a major facility-bill–processing and expense-management company. Eric sits on technology boards for a local high school and community college, was a Microsoft MVP in 2004, and is a moderator on Mark Minasi's Technical Forum.

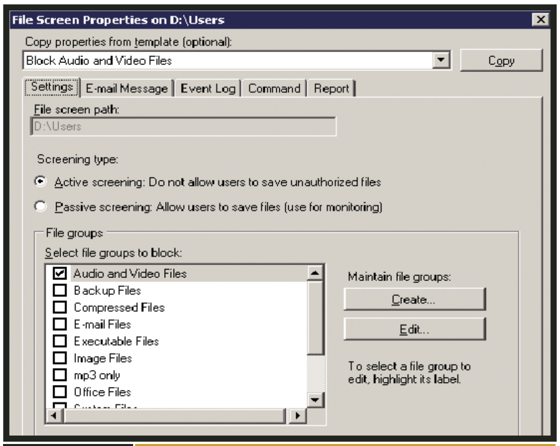


Figure 4: Tuning the file screen

branch, and select File Screens.

3. In the Actions pane, click Create File Screen.

4. Click Browse, and select the path to which you want to apply the file screen. You can then select the template from which you want to derive the settings or set specific values, then click Create.

As Figure 4 shows, after you build a template, you can tune it and define other file types or perform other actions as necessary.

Another type of file screen is possible. The standard file screen is to block file groups, but you can also create a file-screen exception. This capability is useful if, for example, you want to block nearly all file types at a root folder level but create an Audio or Images folder as a subfolder. You can then create file-screen exceptions on those subfolders to allow only audio and images, respectively, thereby forcing data to be stored according to a predefined structure—as opposed to anywhere on disk.

Obviously, there's a small amount of overhead associated with this new technology because the system is performing extra checks. However, the overhead isn't significant: File Screening Management intercepts only write and change operations, and I haven't seen any instances in which file screening has introduced any appreciable bottleneck to system operations.

A Final Caveat

These three common solutions can offer a real benefit to almost any environment. However, a non-technical aspect of these solutions must not be overlooked: communication. Both access-based enumeration and file screening directly affect the end user's experience, and unless communication occurs with users before changes are made, the overall implementation will be seen a failure—no matter how technically successful the implementation is. You never want end-user confusion to ensue and productivity to drop.

InstantDoc ID 94675

John Savill

(john@savilltech.com) is Director of Technical Infrastructure for Geniant and is a CISSP, a Security and Messaging MCSE on Windows Server 2003, a six-time MVP, and a Krav Maga instructor. He is also the author of *Windows Server 2003 Active Directory Design and Implementation* (Packt Publishing)

Get the most from Group Policy with these tried-and-true solutions

GROUP POLICY ANNOYANCES

BY DARREN MAR-ELIA

Group Policy's power is well known. But just as well known are the annoying things about it, when it doesn't always work the way you'd expect. Equally frustrating, the myriad of different capabilities that Group Policy brings—literally thousands of settings—make it tough to know when you can use this technology for a given problem. I've helped many people get the most from Group Policy, and frequently I've seen the same few annoyances cause more than their share of problems. Here's what you can do about them.

Policy Settings Don't Take Effect Immediately

Sometimes it takes two to three reboots for a particular policy setting to take effect. This behavior can be disconcerting because you're not sure whether or not the setting is working. It happens most often for Folder Redirection or Software Installation Group Policy Objects (GPOs), primarily on Windows XP.

This delay is caused by an XP feature called Fast Logon Optimization. In the interests of getting an XP system booted and the user logged on as fast as possible, Microsoft enabled what's referred to as asynchronous foreground Group Policy processing by default. Essentially what this means is that while the computer is starting up, computer-specific Group Policy processing occurs at the same time that the system is working on presenting the logon dialog box to the user. In fact, computer-specific Group Policy processing might still be running when the user enters a username and password and starts to log on. Similarly, when the user logs on, user-specific Group Policy processing starts running and might still be running when the desktop appears. Certain GPO settings—Folder Redirection and Software Installation, for example—need "exclusive" access to the computer or user environment to run. In other words, they need to run synchronously, rather than asynchronously. The Group Policy processing needs to finish doing its thing before the system presents the user with a logon dialog box or the desktop. So how do we tell XP to process GPOs synchronously? By using a policy setting, of course!

Open Group Policy Editor (GPE) and expand Computer Configuration\Administrative Templates\System\Logon to see a policy called *Always wait for the network at computer startup and logon*. Enable this policy for your XP computers, and they'll always run foreground Group Policy processing synchronously. You'll increase the time it takes for a user to boot up a machine and get logged on, but you'll also eliminate the multiple reboot or logon problem when trying to deliver certain kinds of policy. Windows Vista is set to asynchronous processing, just like XP; however, Windows 2000 is set by default to synchronous foreground processing.

Policy Settings Don't Take Effect at All

Sometimes a Group Policy setting doesn't apply at all, and I see 1058 and 1030 event log errors in the Application event log on the client that's having problems. The errors seem to indicate that the system can't read the gpt.ini file. This is a common problem, unfortunately. Because many problems could cause these errors, the best solution is to narrow down the possible causes.

If you notice that this problem occurs only for computer policy settings and not for user policy settings, the cause could be a network-stack timing problem—the computer is booting so quickly that the network stack hasn't had time to initialize fully before the system attempts Group Policy processing, so computer-policy processing fails. However, by the time the user is

Top 6 FAQs about iSCSI

I'm confused by the term Internet SCSI (iSCSI). What is iSCSI and what's its most important use?

The iSCSI protocol encapsulates standard SCSI commands into Ethernet packets for transport over TCP/IP networks. Thus, iSCSI lets you apply network storage solutions in an open environment without using any additional framework, such as Fibre Channel. You can construct a SAN by connecting servers via Ethernet cards (usually Gigabit Ethernet) and iSCSI software initiators or iSCSI host bus adapters (HBAs) and drivers. The servers see the storage as local drives. Like all SANs, you can expand the storage capacity without taking the existing storage offline, so iSCSI is an ideal alternative to more expensive storage solutions that have additional substrate requirements, such as Fibre Channel cards and cable. A major component of iSCSI is its ability to transport, in order, SCSI commands over a network. iSCSI is an attractive alternative for companies that don't want to contend with new hardware alternatives to standard, well-established protocols.

Is cost an issue with iSCSI SAN technology?

The emergence of iSCSI SAN technology, along with ongoing improvements in the disk capacity, performance, and storage-management capabilities of iSCSI storage arrays, has largely eliminated cost as an obstacle to implementing a SAN. An organization can use its existing IP networking equipment to set up a storage array that supports an iSCSI connection. Furthermore, iSCSI SANs, unlike their Fibre Channel counterparts, impose no physical limitations on the distance between the array and the Ethernet switch that connects it to the network.

We're replacing our Exchange Server 2003 servers and are considering booting from Internet SCSI (iSCSI) to a Network Appliance NetApp filer. The new Exchange server will have about 250 mailboxes. Do you have experience booting from an iSCSI adapter in Windows Server 2003? How does it compare with booting from a Fibre Channel Storage Area Network (SAN)?

I've used only the QLogic QLA4010C adapter to boot to an iSCSI array; to my knowledge, this is the only iSCSI setup that currently supports interrupt 13 (INT 13) extensions, which are required for booting. iSCSI offers lower cost and easier implementation at the cost of slightly reduced performance. iSCSI is currently limited to 1Gbps throughput, although some vendors (including QLogic) have pledged support for 10Gbps when such devices are available. Fibre Channel technology typically provides 2Gbps throughput in newer products and 1Gbps in some of the older SAN arrays. Many of the Fibre Channel cards are also available in dual- and sometimes quad-port configurations. The performance improvement probably won't make much difference on an Exchange 2003 server with 250 mailboxes. Keep in mind that backups become a concern when you use a NetApp server to host LUNs instead of using it as a Network Attached Storage (NAS) appliance. You can't restore individual files from LUNs if you use Network Data Management Protocol (NDMP) for backup; you can do so only with NAS. That limitation

continued on back

might not be important, depending on how you want to store Exchange backups for recovery purposes and whether you use Network Appliance's SnapManager for Exchange (which I recommend). I haven't tried connecting a tape library to a SAN array and using multiple SAN cards in a server—one attached to the library and one attached to the array—as you can with a Fibre Channel array setup. But that solution likely would work.

How does iSCSI work?

A server, called the initiator, makes a disk request. The OS and the iSCSI initiator driver intercept the request and encapsulate it in an IP packet. Instead of sending the request to the SCSI bus, the driver directs the request to the NIC, which routes it to the destination address of the iSCSI target (and optionally encrypts it) just as the NIC would do with any other IP packet. When the iSCSI target receives the packet, the target "unwraps" the packet and forwards the enclosed SCSI command to the attached disks. Note that iSCSI, like SANs, transfers data at the block level, whereas Network Attached Storage (NAS) devices transfer at the file level.

How do you create an iSCSI environment?

You need a network, a server or workstation to act as the initiator, the initiator drivers, and a target. The network and initiator computer you should already have; the computer must be running Windows 2003, Windows XP Professional Service Pack 1 (SP1), or Windows 2000 SP3 or later. The initiator drivers are a small, free download from the Microsoft Web site at http://www.microsoft.com/downloads/details.aspx?familyid=12cb3c1a-15d6-4585-b385-befd1319f825&displaylang=en. Installation takes a minute or two, and you don't need to reboot. Installation loads the Microsoft iSCSI Initiator service and an iSCSI Initiator Control Panel applet that has a shortcut on the desktop. The applet offers few configuration options—you enter the IP address or DNS name of the iSCSI target and some security settings.

I understand that we should see an added performance boost by putting Exchange on a 64-bit box. For those of us that connect our Exchange servers to an iSCSI SAN, would we not run into bottlenecks at the NIC (1Gb backbone, assuming we were not using a [TCP/IP offload engines] TOE card or maybe even if we do), before a 32-bit setup cut into performance?

This is a great question, so I'll trot out my all-purpose answer: "It depends." First, let's assume that you have a Gigabit Ethernet connection to the iSCSI SAN, with a host bus adapter (HBA) that has a native x64 driver--no thunking required. That's just a clarification, but in the end it doesn't really matter. Why? Assuming that you have enough RAM, the Exchange Server 2007 implementation of the JET database engine will be able to cache a significantly larger portion of the EDB file than it can now. Therefore, the amount of bandwidth between your server and the iSCSI cabinet becomes much less relevant. What about page size? My gut feeling is that the page size change will be a wash; caching will reduce the total number of I/O operations per second (IOPS) that have to go over the wire, but those pages that do go will be 8KB instead of 4KB. Why did I say "it depends," if the performance news is so rosy? Because one of the key reasons people will be deploying Exchange Server 2007 is to consolidate servers. Obviously, if you take four or five Exchange Server 2003 servers and stuff their mailboxes onto an Exchange 2007 server, the new server will require a significant amount of SAN bandwidth, and I suspect it'll easily be possible to build configurations that would saturate a Gigabit Ethernet HBA. So, don't do that and you should be good to go!

ready to log on, the stack is up and running, so user-policy processing works just fine.

Microsoft added a nifty little registry entry to certain versions of Windows, which you can use to tell the system to wait until the network stack is finished initializing before Windows starts policy processing. This registry entry is described in the Microsoft article "Group Policy application fails on a computer that is running Windows 2000, Windows XP Service Pack 1, or Windows XP Service Pack 2" (http://support.microsoft.com/?kbid=840669). You'll also find it as a GPO setting in Windows Vista, under Computer Configuration\Administrative Templates\System\Group Policy*Startup policy processing wait time*.

Other problems might cause these error messages. For example, perhaps the gpt.ini file really is inaccessible. This file is stored in the part of a GPO stored in the SYSVOL share on each domain controller (DC) in your environment. When the system performs either computer- or user-specific Group Policy processing, it needs to read this file to get information about the GPO. If the file isn't present on the DC the system is reading from, Group Policy processing will fail. You can verify which DC is servicing Group Policy processing by looking in the HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Group Policy\History\DCName registry value.

After you identify the DC in question, verify that SYSVOL is actually shared out, that the DFS service is running on the DC (SYSVOL uses DFS replication), and that the TCP/IP NetBIOS Helper Service is running on the client (the client uses this service to communicate with DFS). From a command shell on the client, you can type

```
net view \\<DCname
```

to verify that SYSVOL is shared, and use the netstart command to verify that all required services are running. Also browse to the file location that showed up as inaccessible in the event log entry and verify that the file is actually there and that the file's permissions are the same as on another DC where you know policy is working.

For permission problems, Group Policy Management Console (GPMC) might be able to help. Open GPMC focused on the DC that's having a problem. To do this, change GPMC's DC focus by right-clicking the domain name and selecting Change Domain Controller, as Figure 1 shows. After you've focused GPMC on the problem DC, go to the Group Policy Objects container and select the GPO that's having problems. If GPMC spots permission problems on that GPO, GPMC will prompt you and offer to fix them.

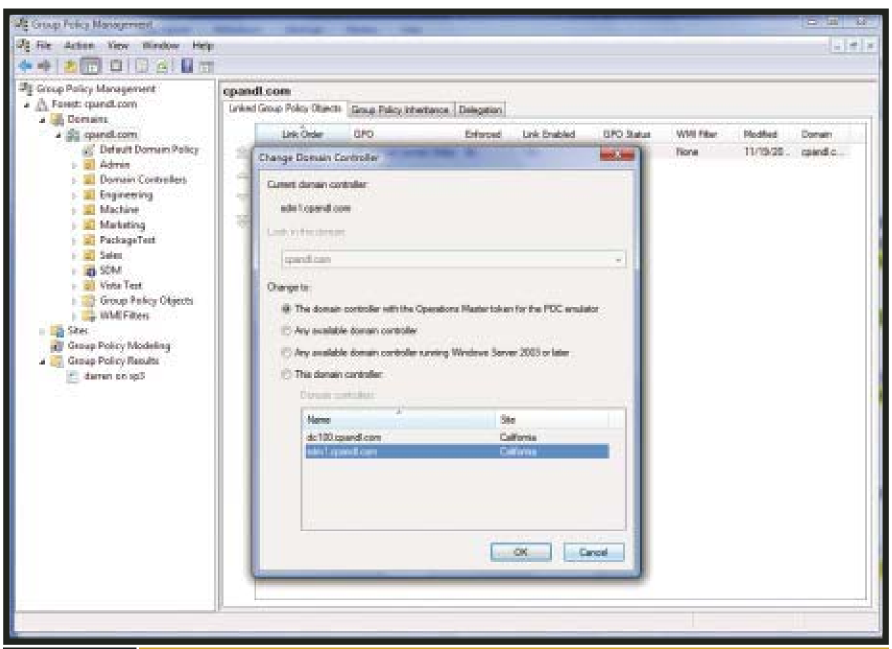


Figure 1: Changing domain controller focus

Loopback Policy Is Confusing to Implement

If you're working in the Terminal Server component of the Windows Server 2003 environment, you want to be able to deliver different policy settings to users when they log on to the terminal server versus when they log on to their desktops or laptops. This scenario is exactly why loopback policy was created, but the policy can be confusing to implement.

Loopback policy says, when I'm logged on to a particular computer that has loopback enabled, deliver user policies that are defined for the computer object, rather than the user object. The easiest way to implement loopback policy is to put your Terminal Server computer objects into their own organizational unit (OU) within Active Directory (AD). Then create a GPO and link it to that OU. Within that GPO, enable the policy under Computer Configuration\Administrative Templates\System\Group Policy*User Group Policy loopback processing mode*. This policy enables loopback processing for the computers in that OU. You might typically want this for "kiosk" or public-use computers, where you want a machine to behave a particular way regardless of who logs on to the machine.

The policy has two modes: merge and replace. The mode you choose will depend upon what you're trying to accomplish. Merge mode says, first run my regular user policies when I log on to the Terminal Server box, then run the computer-based user policies. Should the regular user policies and the computer-based user policies conflict, the computer-based policies prevail because they're processed last. Replace mode says, don't even process my regular user policies—just process the computer-based user policies.

In my experience, replace mode is simpler to manage and should be used unless you need some of the user's regular policies to apply when the user logs on to the Terminal Server system. Note that if you use merge mode, some policies might run twice when the user logs on to the terminal server. For example, if you have logon scripts defined at the domain level, the scripts will apply to both the user object and the computer object, and because the computer object is running in loopback merge mode, the system will process those logon scripts once for the user object and again for the computer object.

Make sure you enable loopback processing so that it affects only those computers that really need it (hence my recommendation to

enable loopback policy on a specific OU that contains only loopback computers). If you enable the policy more generally, you might get unexpected results whose cause can't be detected because you enabled the policy by setting a particular registry value that isn't exposed in any reporting.

Group Policy Provides Potentially Conflicting IE Settings

With the release of XP Service Pack 2 (SP2) and Windows Server 2003 SP1, Microsoft put into the Administrative Templates policy many Microsoft Internet Explorer (IE) settings that seem to conflict with or at least overlap what's found in IE Maintenance policy (under User Configuration\Windows Settings\IE Maintenance Policy). So where should you configure IE policy?

Unfortunately, there's no clear answer, but you should take note that Microsoft is moving IE configuration toward Administrative Templates–style settings and de-emphasizing IE Maintenance features. Basically, the reason for this move is Microsoft's poor implementation of IE Maintenance when the policy was first created. The IE Maintenance policy area has had many bugs and is generally difficult to use.

Still, you absolutely have to use IE Maintenance policy to do such things as setting the browser proxy settings, or Favorites. But for IE security configuration, your best bet is to ignore IE Maintenance and use the Administrative Templates policies found under User Configuration\Administrative Templates\Windows Components\Internet Explorer. For example, if you need to configure trusted sites for a particular zone, you can use the *Site to Zone Assignment List* policy under User Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel\Security Page. You can also set individual zone security settings (visible at the IE Internet Options, Advanced page) within User Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel\Security Page\Internet Zone, Intranet Zone, etc. A cautionary note: Avoid setting IE security policy in *both* the IE Maintenance and Administrative Templates sections, as their interactions can be unpredictable.

Also, IE Maintenance has this annoying feature: If you're defining a GPO such as Connections Settings to set up a proxy, IE Maintenance imports those settings from the machine on which you happen to be editing that GPO at the time. So if you set a policy for settings on one machine, then go to a machine whose IE connection settings are different, when you click the button to modify settings, you'll see the new machine's settings and not those from the first machine where you were editing that GPO. This can cause no end of problems. For that reason, if you have to use IE Maintenance policy, always try to make subsequent edits to that policy from the machine on which you made your original changes (provided you haven't changed IE's configuration since the last time you edited that policy).

Removing a Machine from a Domain Won't Erase GPO Settings

Sometimes you just want to wipe the slate clean and remove all GPO settings that have been applied to a particular user or computer. For example, let's say you're going to move a computer out of an AD domain into a workgroup and you no longer want Group Policy enforced on it. In that scenario, you must follow a specific set of steps *before* you remove the machine from the domain. You can't just remove the machine from the domain, because any GPO settings set on that machine will be "orphaned" on the machine and you won't be able to easily remove them, as those settings came from domain-based GPOs that no longer exist in the workgroup.

Therefore, before you remove the machine from the domain, move the machine's account in AD to an OU that has no GPOs linked to it (and make sure to block any upstream GPOs by using the Block Inheritance flag on that OU). Then reboot the computer. For most policy settings, what will happen is that during the Group Policy processing cycle that happens at reboot, the machine will notice that none of the GPOs that it had previously applied are applicable anymore, and so those settings that can be removed (e.g., Administrative Template policy, Software Installation policy) will be removed during this processing cycle.

After the machine is "clean," you can safely remove it from the domain. The only caveat to this method is that some policies, such as security settings configured under Computer Configuration\Windows Settings\Security Settings, won't be removed because Group Policy doesn't know what their default state was. In that case, you can use the secedit.exe command-line utility to apply the baseline security template that was in place when you first installed Windows. This baseline is called setup security.inf and can be found in C:\windows\security\templates in XP Professional and Windows Server 2003. You can easily use this template to reset security by opening the local GPO Editor (type gpedit.msc from the Start menu Run dialog box) and navigating to Computer Configuration\Windows Settings\Security Settings. Right-clicking that node, choose Import Policy from the menu and then select the setup security.inf file to import.

There's no doubt that Group Policy is complex—with lots of moving parts and interdependencies to complicate a powerful configuration-management system.

You'll Never Walk Alone

I hope this list touched on many of the problems you've had with Group Policy and provided some fresh answers to help solve them. There's no doubt that this stuff is complex—with lots of moving parts and interdependencies to complicate a powerful configuration-management system. Just know that you're not alone when it comes to struggling with some of these problems.

InstantDoc ID 94618

Darren Mar-Elia

(dmarelia@windowsitpro.com) is a contributing editor for *Windows IT Pro* and is CTO and founder of SDM Software. He maintains a Group Policy resource Web site (http://www.gpoguy.com) and is coauthor of *Microsoft Windows Group Policy Guide* (Microsoft Press).

DNS ANNOYANCES

BY MARK BURNETT

Quick answers to common problems

Although DNS services are fundamentally simple, certain problems frequently appear. Quite often, unclear wording or poorly documented options in various Windows dialog boxes can cause these problems. Let's look at some common DNS annoyances that plague administrators and how you can deal with them.

Dynamic Updates Won't Update

Windows allows clients to dynamically update A and PTR records with DNS servers to help simplify DNS management across a domain. Thus, in an AD-integrated zone, when you assign IP addresses in your organization, client machines can dynamically update AD with their new IP address. Sometimes, however, you might notice that client systems aren't properly updating their DNS records with the new address. To make updating work, you must configure the DNS server to allow dynamic updates. To do so, open the properties for the DNS zone and select *Secure only* for the *Dynamic updates* setting, as Figure 1 shows.

Next, on the client, open the network adaptor's Advanced TCP/IP Settings dialog box, select the DNS tab, as Figure 2, page 36, shows, and make sure that *Register this connection's addresses in DNS* option is selected.

Finally, the DHCP client service—not just the DNS client service—handles DNS registration and must run on each system. Even if you don't use DHCP to assign IP addresses, you need the DHCP client service to run on each machine to dynamically update DNS records.

By default, a client will update DNS records upon start-up, or when an IP address or name changes, or when you force it to update by using the ipconfig /registerdns command. Furthermore, the client will reregister its IP address every 24 hours.

DNS Client Service Causes Performance Hits

When the DNS client service starts, it loads all entries in the hosts file to its cache. If you use a very large hosts file to block access to unwanted host names, you might find that this service significantly slows system performance. In such a case, you might want to disable the service.

However, typically, disabling the DNS client service will have no effect on DNS lookups. You might wonder, then, why anyone would need this service in the first place.

The answer is that the DNS client service isn't *necessary* for name resolution; it just makes name resolution smarter and more efficient. The main purpose of the DNS client service is to provide local caching of DNS entries. The service is, in effect, a DNS server itself. Instead of publishing a database of DNS records, it simply caches previously resolved DNS records to speed up future lookups. Besides caching, the service optimizes network connections by prioritizing resource records based on network location, speed, and availability.

The DNS client service also manages the list of DNS servers configured on a system. As it does with resource records, the service selects the best DNS server from the server list, based on network location, speed, and availability.

Firewall Rules Need to Be Optimized

When you configure a firewall to allow public requests to a DNS server, you want to build rules that won't let others exploit your configuration. DNS queries typically come in on UDP port 53 from a source port greater than 1023. The DNS server responds from source port 53 to the same port used by the client. Most stateful firewalls can handle DNS responses, so a single rule governing requests should be enough.

If a query response is greater than 512 bytes, the DNS server indicates to the client that the response is truncated. The client can resubmit

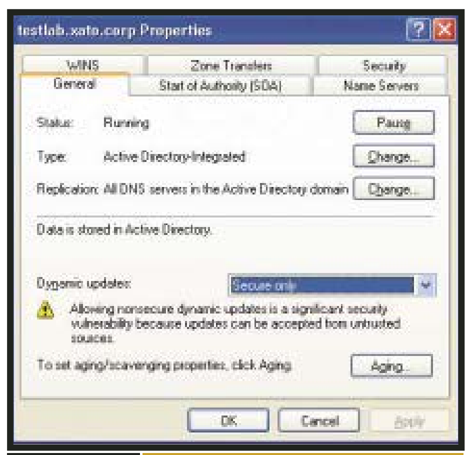


Figure 1: Configuring the DNS server to allow dynamic updates

the query using Extended DNS, which allows for larger UDP responses, or the client can resubmit the response by using TCP. If you allow TCP queries, you'll need a rule that allows packets coming in on TCP port 53 from a source port greater than 1023. If you know that your DNS server won't return query responses larger than 512 bytes, you can leave this port closed. Some DNS servers use UDP or TCP port 53 as both their source and destination port for server-to-server queries, so you might also need to configure your firewall to allow this.

How Windows Queries Multiple DNS Servers

By default, Windows first queries the first listed DNS server on the primary network adaptor. If this server doesn't respond within one second, Windows sends the query to the first listed DNS server on any other network adaptors on the system. If it receives no response within two seconds, Windows sends the query to all DNS servers listed on all network adaptors on that system. If none of these servers respond in two seconds, Windows sends the query to all servers again and waits four seconds. If necessary, it resends the query to all servers and waits eight seconds.

Windows adjusts the list of DNS servers it queries depending on network conditions. If none of the DNS servers on an adaptor reply to queries, Windows assumes a network failure has occurred and doesn't query any servers on that adaptor for 30 seconds. If one DNS server on a network adaptor returns a negative response to a query, Windows won't resubmit that query to any other DNS servers on that adaptor. Furthermore, Windows might adjust the order in which it queries DNS servers to favor a server that responds more quickly than others.

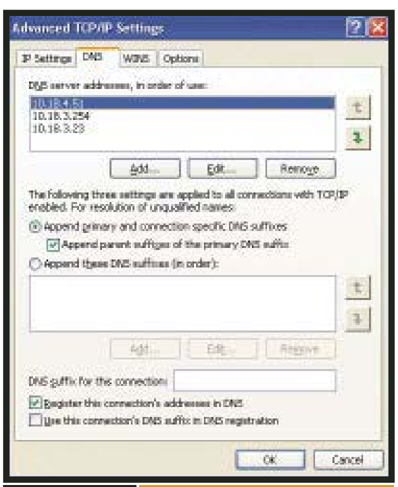


Figure 2: Configuring the client to register a connection's address in DNS

GUIs Slow Configuration

If you do a lot of DNS server configuration for client systems, you'd probably like a quicker, easier method than using the Windows GUIs. Try these commands at a command prompt. To list all of a client's DNS servers, type

```
c:\>netsh interface ip
 show dns
```

To clear the list of DNS servers for a network adaptor where "Local Area Connection" is the name of that network adaptor, type

```
c:\>netsh interface ip
 set DNS "Local Area Connection"
 static none
```

To add a DNS server for a network adaptor where "Local Area Connection" is the name of that network adaptor, type

```
c:\>netsh interface ip
 set DNS "Local Area Connection"
 static 192.168.0.1
```

Domain DNS Problems

Misconfigured DNS settings are a common source of problems with Windows domains. A quick way to check your settings is to perform a lookup for the domain name itself, which you can do with this command:

```
c:\>nslookup <yourdomain>
```

The command should return a list of IP addresses that point to each of your DCs. If you get anything else, check your DNS configuration.

You can also test your DNS configuration by performing a quick network configuration test on any Windows XP or Windows Server 2003 system. From a command prompt, type

```
c:\>netsh diag show test
```

This test pings all DNS servers and gateways in your TCP/IP configuration. If you have the *Microsoft Windows Server 2003 Resource Kit*, you can use the netdiag or dnsdiag commands instead, as follows:

```
C:\>netdiag /test:dns
```

or

```
C:\>dnsdiag
```

If you want to test your public DNS servers from the outside, you can use either one of these URLs: http://www.dnsreport.com or http://www.dnsstuff.com. To test to see if a remote DNS server allows zone transfers, use this command:

```
c:\> echo ls -d <targetdomain>
 | nslookup - <nameserver>
```

If the name server allows zone transfers for that domain, it will return all records in the zone. Otherwise, it will return an error.

BIND Is an Acronym, Not a Verb

In a DNS server's properties dialog box, you'll find the BIND Secondaries setting. BIND isn't a verb—it's an acronym for Berkeley Internet Name Domain, which is an implementation of DNS used for handling DNS requests on the Internet.

When performing zone transfers, the DNS server uses a faster zone transfer method that utilizes compression and can transfer multiple records per TCP message. This format isn't compatible with older versions of BIND. You need to select the BIND Secondaries option if you use a version of BIND earlier than 4.9.4. This option tells the Windows DNS server not to use the faster zone transfer methods.

When to Disable Recursion

Recursion is the process that DNS uses to track down the authoritative server for a domain. If you query a DNS server for a host in a domain and the server isn't authoritative for that domain, nor does the server have a cached copy of the requested host record, the server recursively queries other servers on the Internet on your behalf to track down the DNS server with the correct answer. If a server doesn't do recursion, it either tells the client it doesn't know that record or it tells the client where it might find the record.

To determine when you should disable recursion, you need to look at what types of records the DNS server will hold. If the DNS server for a domain knows all the records for a domain, it should never provide recursion. Your DC, for example, knows about every host in your domain, so there's no need for it to send a request elsewhere. The same is true for a public DNS server that holds published domain records.

You should typically allow recursion on servers that provide DNS lookups for local users.

That is, if you provide Internet access to a user, you should also provide that user with a recursive DNS server that can resolve any Internet host name.

It's important not to make recursive DNS servers available outside of your organization. A server could be attacked and used as an amplifier for Distributed Denial of Service (DDoS) attacks.

Internet Host Blocking

Here's a problem that DNS isn't responsible for but that it can partially help you solve. You can block user access to undesirable Internet hosts by using a firewall or a proxy server, but those solutions don't work well for all situations. An ISP, for example, might want to block certain host names without requiring customers to use a proxy server and without putting too much of a load on the firewall. Blocking host names at the DNS server is one alternative.

To do this, you first need a list of hosts to block. You can get a malware block list formatted for Microsoft DNS servers from Malware Block Lists at http://www.malware.com.br/#blocklist. You can directly import this block list into your DNS server. If you're willing to do some reformatting, you can also get block lists from hpHosts Online at http://www.hosts-file.net or Spamassassin Blacklists at http://www.sa-blacklist.stearns.org/sa-blacklist.

Another alternative is OpenDNS (http://www.opendns.com), a free DNS service that provides filtering by blocking known phishing hosts. To use OpenDNS, you just place its DNS server IP addresses in your network configuration.

Keep in mind that using DNS for blocking only prevents name lookups for hosts on these lists. It doesn't prevent users from accessing hosts by entering their IP address, and it can't block new hosts that haven't yet been listed.

Learn the Fundamentals

DNS problems generally have simple solutions, but you do need to have a good understanding of how DNS works. Expand your knowledge of DNS—for any IT professional, it's certainly time well spent.

InstantDoc ID 94456

Mark Burnett

(mburnett@xato.net) is an independent security consultant and author who specializes in Windows security. He is an IIS MVP and the author of several books, including *Perfect Passwords and Hacking the Code* (Syngress).

More DNS Tips

People frequently approach me for help with their questions about the peculiarities of DNS. Here are a couple things you might want to know about using DNS.

Using Both Round-Robin Rotation and Netmask Ordering

Windows DNS servers let you enable both round-robin rotation and netmask ordering features. Often a host name such as www.microsoft.com has multiple IP addresses to improve load balancing and performance. These IP addresses might be multiple paths to a single server or point to geographically dispersed servers.

To load-balance DNS requests, a DNS server uses round-robin rotation to move through a list of IP addresses, effectively distributing traffic evenly among different servers. With netmask ordering, the DNS server attempts to return the host IP address that's physically closest to the client. The DNS server does this by looking at the first few octets of an IP address, assuming that a server with an IP address similar to a client will most likely be physically closer to the client. By default, the DNS server gives priority to any host address in the same class C network as the client.

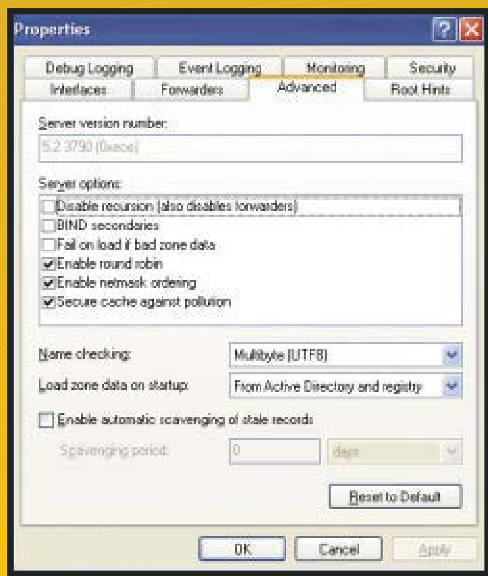


Figure A: Enabling round robin and netmask ordering

Although it might seem like round robin and netmask ordering wouldn't work together, as you can see in Figure A, Windows lets you use both features at once. If you select both methods, Windows checks a host's list of IP addresses to see whether an IP address on the list closely matches the client's IP address. If Windows finds a match, it will give that IP address a higher priority for the round robin. The result is that the DNS server performs a round-robin rotation of IP addresses, but the round robin is biased toward returning the server that appears to be closest to the client.

Integrating DNS with Active Directory

When you install DNS on a Windows domain controller (DC), you have the option of storing your zone files in the Active Directory (AD) database rather than in simple text files. You might wonder why you would choose to integrate a zone with AD.

In most cases, integrating DNS zones into AD provides many benefits, the primary one being improved replication. In AD-integrated zones, AD securely automates replication of DNS records among servers. AD replication is multimaster replication, meaning that you can make a change on any DC and the change is automatically propagated across the domain. For DNS zones that aren't integrated with AD, you must set up primary and secondary DNS servers. Then when you make changes, you typically make them to the primary server, which updates all secondary servers.

InstantDoc ID 94630

Get the answers you need to 6 big security problems

SECURITY ANNOYANCES

BY RANDY FRANKLIN SMITH

Trying to keep your company's information secure is a lot of work and is unlikely to make you popular with users. Typically, the tighter you try to lock down a network, the more hassle the network is to administer as repetitive tasks become necessary for both end users and you. But there are ways to ease the pain—often by deploying automation technology. Let's look at six common security annoyances and practical, effective ways to overcome them.

Password Resets

Resetting passwords for users who forget them is the bane of every administrator. A META Group survey indicates that this thankless task alone costs companies with 10,000 users well over half a million dollars a year (http://www.microsoft.com/technet/security/guidance/identitymanagement/idmanage/p2pass.mspx). But there are ways to reduce or even eliminate this problem. My favorite solution is to use electroshock therapy. With a few simple modifications to a keyboard's wiring and a device-driver hack, you can deliver 120 volts of behavior-changing juice to the nervous system of your users when they enter their passwords incorrectly. A couple of jolts and your problem is solved!

You can train users to remember passwords with less violent behavior-modification methods. The most effective password-memorization technique I've found is creating passwords by using the first letter of each word of a sentence that the user can remember. You'll need to use a sentence that has some proper nouns and numbers so that this technique produces a complex password with upper-case letters and nonletter characters. You can let users come up with their own sentences, but I've had better success assigning users passwords based on a sentence of my choosing. Assigning passwords this way carries the added benefit of the enjoyment you get by forcing users to mentally recite your brutally honest observations about their personality or appearance. Of course, if you have one of those irksome corporate security policies that says you shouldn't know everyone's password (like you can't just run a password cracker, right?), then you might have to look at other alternatives.

Enter the automated password reset tool. Let's think about it. Resetting a user's password is a pretty mundane, clerical process: Authenticate the person requesting the password reset, find his or her account, and reset its password. Why not automate this? A variety of self-service password reset solutions are already on the market to take this burden off your shoulders, and it's not hard to justify the cost when you consider the savings in IT staff time. Solutions on the market provide various methods for letting users reset their own passwords, from Web-based applications to telephone-based systems. Some of the players include Avatier Password Station and M-Tech Information Technology's P-Synch. Just do a Web search for "password reset self-service" and you're on your way.

Protecting Laptop Data

Protection of laptop data is receiving increasing scrutiny from legislators and the media. When an organization loses a laptop containing customers' personal information, the organization is in for some hefty unexpected costs associated with notifying each customer of the security breach as well as the more-difficult-to-quantify costs of bad press and loss of good will.

I've watched this problem and the technologies designed to address the risk of stolen or lost laptops for years. Many solutions have caused more problems in terms of stability or administration than they were worth. Other solutions slowed down systems or were too impractical because they depended on users to encrypt or decrypt files or manage encryption keys. I've used Windows Encrypting File System (EFS) for my clients, but drawbacks and

instance, EFS doesn't support whole-volume encryption, so data can leak out from unencrypted folders.

Windows Vista's new BitLocker Drive Encryption feature for whole-volume encryption and its integration with the Trusted Platform Module (TPM) found in most business laptops today provides the best all-around solution for protecting data on laptops. In fact, I'd say BitLocker is the single biggest motivator for migrating your laptop fleet to Vista.

With BitLocker, you divide your hard drive into two volumes. One volume is very small (just a few megabytes) and initially left empty; you install Vista to the partition that occupies the rest of the drive. Then you enable BitLocker and wait for it to encrypt the entire large volume. BitLocker installs a bootstrap loader on the small volume, which is protected from tampering by the laptop's TPM. When the laptop is turned on, the TPM checks, through hashes stored in its tamper-resistant memory, whether the tiny bootstrap partition has been modified. If it hasn't, the TPM allows the bootstrapper to load. The bootstrapper retrieves the encryption key for the larger volume from the TPM and proceeds to boot Vista on the larger, encrypted volume. This description is a bit simplified, but the bottom line is that for the first time, we have laptop hardware, tamper-resistant key storage, and whole-volume encryption all integrated with the OS for the most transparent, best performing, and effective encryption solution I've seen to date. To learn more about BitLocker, see the Windows BitLocker Drive Encryption Step-by-Step Guide (http://www.microsoft.com/technet/windowsvista/library/c61f2a12-8ae6-4957-b031-97b4d762cf31.mspx).

BitLocker is the single biggest motivator for migrating your laptop fleet to Vista.

Lovely Spam, Wonderful Spam

Spam is such a pain. Kind of the understatement of the decade, eh? We all hate it, and it's a security threat because we can all too easily open an attachment containing a virus.

If you aren't careful, though, your antispam solution can become an even bigger pain. No antispam solution is 100 percent accurate. You run two basic risks with an antispam solution: user dissatisfaction with low catch rates and user dissatisfaction with false positives, both of which lead to increased care and feeding of users by IT staff (i.e., support calls).

In my experience, an 80 percent catch rate for spam is pretty reasonable; users shouldn't expect much better unless they're willing to regularly hunt down good email messages that got caught by the spam filter. Many antispam solutions claim a much higher catch rate but don't mention their false positive statistics. Moreover, catch rates vary from organization to organization, and even user to user, because of the content and phrases peculiar to different industries and what each user considers to be spam. A marketing professional may have a view of spam very different from a technician who doesn't have much interaction outside the organization.

In my opinion, Sender Policy Framework (SPF) spam detection has the best potential to significantly reduce spam, but too few companies have taken the time to publish an SPF record for their DNS domain. An SPF record published in your domain's zone file formally declares the official SMTP servers for your domain so that other organizations can determine if email that purports to be from your domain really is. Don't delay: There are great setup wizards on the Internet that will help you build your own SPF record—for instance, http://www.openspf.org.

As seductive as the idea of a Bayesian-based, "self-learning" antispam solution is, I've had better luck with frequently updated signature-based spam-detection solutions. Like antivirus solutions, signature-based spam-detection solutions require the vendor to constantly monitor messages, quickly update their signature database, and just as quickly push the updated file to their customers. Microsoft Exchange Intelligent Message Filter (IMF) would be a much better solution if Microsoft updated it more frequently. I always see a dramatic drop in spam after I install an IMF update, but the amount of uncaught spam immediately begins to climb. Other signature-based spam solutions, such as St. Bernard Software's ePrism, are much more frequently updated. There are also a number of antispam services available that relieve you from installing and maintaining any software by routing your mail through the antispam service's servers first.

Perhaps the biggest risk in implementing an antispam solution is the potential increase in support calls from users trying to find email messages that were apparently eaten by the antispam solution. Any solution that requires you to get involved when a user needs to retrieve a false positive is more trouble than it's worth. My advice is to install only antispam solutions that make all email identified as spam easily accessible to the user—preferably without leaving the email client. As examples, you can configure both IMF and GFI Software's GFI MailEssentials to put all spam into the recipient's junk email folder. Even better, GFI MailEssentials lets you specify a different folder for each antispam method it supports, so you can determine which method (e.g., Bayesian, SPF, Realtime Blackhole List—RBL) is responsible for misclassifying a good email message by the folder in which it ends up.

Wi-Fi Security

Most organizations I run into are still using Wired Equivalent Privacy (WEP) standard or Wi-Fi Protected Access (WPA) pre-shared keys to secure their wireless LANs (WLANs). WEP isn't secure no matter how strong your shared key is due to vulnerabilities in the protocol and associated algorithms. WPA and WPA2 pre-shared keys are secure only if they are at least 22 characters long and drawn from a large character set. Long shared keys, though, are an annoying, time-sapping problem for IT staff and users because of all the management and security issues that arise. Users can't remember them, so you're constantly asked for the key, and frighteningly few users seem capable of typing more than a few characters correctly in sequence. Whenever a new computer is commissioned or a contractor comes in, you must get them access to the WLAN. And what happens if a pre-shared key is compromised?

The solution is elimination. Get rid of WPA with pre-shared keys (WPA-PSK). No, not WPA altogether—just the PSK part. Implement 802.1x in place of pre-shared key authentica-

tion. With 802.1x, you configure your Access Points (APs) to interface with Active Directory (AD) via Remote Authentication Dial-In User Service (RADIUS) to authenticate users and computers based on their AD credentials. You have to install Internet Authentication Services (IAS) on one of your Windows servers, such as a domain controller (DC); IAS is Windows' built-in RADIUS server. After installing IAS, you introduce the APs and IAS to each other with some simple configuration settings, and in no time your Windows wireless clients will begin authenticating to your WLAN by using either the computer's or the user's credentials.

By applying a few Group Policy settings, you can make the authentication process transparent to users of computers that belong to your domain. Outside users such as contractors and consultants that need access to your WLAN simply need to enter the user name and password of an AD account that you provide them. IAS allows you to limit access to WLAN and internal wired networks based on group membership, which allows you to restrict external consultants to Internet-only access, for instance. For detailed directions for implementing 802.1x on your WLAN, see the *Windows IT Security* article "Reaping the Benefits of WPA and PEAP," June 2006, InstantDoc ID 50105. By replacing WPA-PSK with 802.1x, you leverage the user accounts you already manage in AD and eliminate the headaches of pre-shared keys.

Restoring Files

Backup and recovery is very much a part of information security, even if it isn't the first thing you think of. There's nothing more annoying than being close to a new high score on your favorite computer game when an inconsiderate user calls up whining about a file he needs restored. While mourning your dead game avatar, you must rouse from the comfortable environs of your cubicle, find the appropriate tape, restore the file, inform the user, and repeat the process when he decides he really needed a version from a week earlier.

Stop the insanity! Get Microsoft System Center Data Protection Manager (DPM), and put users in control of their own restores—right from Windows Explorer. After you install a DPM server and the associated agent on your file server, DPM periodically takes snapshots of your server. It efficiently stores multiple versions of each file in its online Microsoft SQL Server database. After you push out a necessary hotfix explained in the Microsoft article "How to use the End User Recovery functionality of Data Protection Manager in Windows XP" (http://support.microsoft.com/kb/895536) to your Windows XP clients, users will be able to browse available backup versions of any file on the server directly from Windows Explorer.

Failing to solve problems and automate tasks leads to a less and less productive IT department.

To facilitate offsite backups of your data, DPM lets you back up shadow copies of your file servers from the DPM database, giving you a disk-to-disk-to-tape backup scenario. To learn more about DPM, go to http://www.microsoft.com/systemcenter/dpm.

Patch Management

Patch Tuesday is many administrators' least favorite day of the month. And zero-day vulnerabilities are rearing their ugly heads more frequently between Patch Tuesdays. I have three recommendations for making your patch-management effort less of a nightmare:

- Life is too short to push out patches manually. Implement Windows Server Update Services (WSUS) or another automated patch-management solution. WSUS is free, but many excellent ISV offerings go beyond WSUS's functionality, providing broader platform and application support and better manageability, including those from St. Bernard Software, PatchLink, BigFix, Shavlik Technologies, and ScriptLogic.
- Many administrators are reluctant to push out a patch without testing it, but testing is time-consuming and annoying. In addition, the user community usually identifies defective patches soon after their release. Organizations with a small IT staff might consider just sitting on patches a couple of days and monitoring for any advisories or revisions from Microsoft, then deploying them without testing.
- An especially annoying type of vulnerability is that for which no patch is available—zero-day vulnerabilities. Most zero-day exploits are related either to a specific file type (e.g., .doc, .xls, .ppt, .bmp, .png) or to a Microsoft Internet Explorer (IE) ActiveX object. More and more antivirus vendors quickly release signature updates for file-format exploits even though they aren't, strictly speaking, viruses. If you cover your file-borne vectors (principally email attachments and Web downloads) with multiple antivirus engines, you'll often be protected against these file-borne zero-day exploits well ahead of patch availability. The easiest way to address ActiveX-related vulnerabilities is to set the kill bit on the ActiveX control. I've created an administrative template that you can use with Group Policy to automatically set the kill bit for an ActiveX control on thousands of computers in a short time. The template and a video demonstrating how to set it up can be found at http://www.ultimatewindowssecurity.com/killbit.asp.

Take Action

In the case of many security annoyances, the key is to automate or implement newer technologies, but often such projects are put off because of the initial setup involved or the purchase costs. However, failing to solve problems and automate tasks leads to a less and less productive IT department that moves in slower and slower motion, dragged down by outdated, manual procedures. The IT department that succeeds in climbing the steep, initial curve to eliminating IT headaches such as those in this article will reap the benefits in the long run. A few weekends at the office now can save you many evenings and weekends in the future.

InstantDoc ID 94414

Randy Franklin Smith

(rsmith@ultimatewindowssecurity.com) is a contributing editor for *Windows IT Pro*, an information security consultant, and CEO of Monterey Technology Group. He teaches Monterey Technology Group's Ultimate Windows Security course series and is an SSCP, a CISA, and a Security MVP.

Q: I want to create a site-to-site VPN connection from our branch office to the corporate datacenter by using RRAS on our Windows server. Our basic broadband firewall/router supports pass-through for outgoing PPTP connections, and I think I've correctly configured the site-to-site VPN on the RRAS servers at the branch office and at the datacenter. But I don't know how to get the PCs on our branch network to use the RRAS server when they want to communicate with servers at the datacenter and the firewall when accessing the Internet. In many scenarios, the VPN server is also the router connecting the LAN to the Internet. In our case, I can't replace the router with a Windows server because of other policies. How can I solve this problem?

A: You need to do two more things. First, you need to configure your router/firewall to route traffic destined for the datacenter and local branch network through your local RRAS server instead of directly over the Internet. To do this, you need to know the subnets at the datacenter to which your local computers need to communicate. Then you add some router rules to the firewall so that it sends packets addressed to those subnets to the VPN server instead. While setting up your site-to-site VPN using Windows Help you should have already added one or more static routes for the same subnets that route such traffic over the VPN connection. Figure 1 shows a screen print of the route defined on my local firewall that routes traffic destined for my other office through 10.42.42.40—the address of my local VPN server.

With that rule configured, whenever the router sees a packet destined for your datacenter, it will relay the packet to your local RRAS server. The RRAS server encapsulates it into a PPTP packet and sends it back to the firewall and out over the Internet. For what it's worth, you could have reconfigured your branch DHCP server to configure DHCP clients to replace the router as the default gateway with your RRAS server. Then the RRAS server would receive each packet first and route it directly to the Internet via your firewall or first through the VPN connection, as appropriate. I prefer to keep the router as the default gateway because if the local RRAS server goes down, users can still access the Internet, which wouldn't be the case if the RRAS server were the default gateway.

You'll also probably need to change how DNS queries are resolved by computers at your branch office. Currently, your DHCP server is no doubt configuring computers to use the router as their primary DNS server. Therefore, DNS queries for servers at your datacenter will go unresolved unless you can configure your firewall to try resolving DNS queries first against an internal DNS server at your datacenter via your site-to-site VPN. But more likely, you'll need to configure your local RRAS server as the primary DNS server for your branch LAN. After you install DNS on your RRAS server, you'll create two forwarding entries so that the server first forwards all DNS requests to an internal DNS server at the datacenter, then forwards any unresolved queries to your firewall. You'll also want to configure your DHCP server to specify your firewall as the alternate DNS server for the branch LAN. Then if your RRAS server goes down, branch computers will still be able to get DNS queries for Internet sites resolved, preserving Internet access.

InstantDoc ID 94647

—Randy Franklin Smith

Q: Does Windows Vista offer a way to easily start frequently used applications?

A: Vista introduces keyboard shortcuts that let you easily start frequently used programs. First, add the program's shortcut to the Quick Launch toolbar. Then, simply press the Windows logo key plus a number. For example, to start the first shortcut on the Quick Launch toolbar, press the Windows logo key+l; to launch the second shortcut, press the Windows logo key+2, and so forth.

—John Savill

InstantDoc ID 94773

John Savill
john@savilltech.com

Randy Franklin Smith
rsmith@
ultimatewindows.com

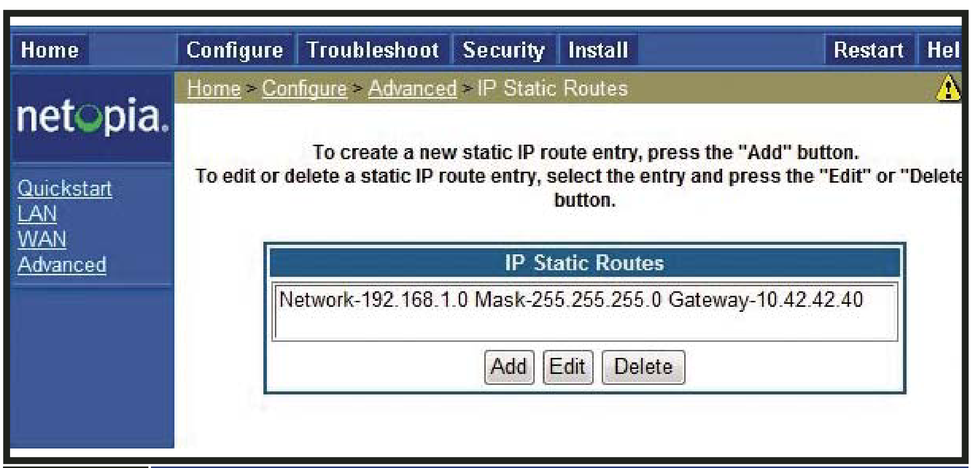


Figure 1: Routing branch office traffic through a local VPN server

At a Glance

…Tired of Nursing Your Exchange Server?

#1 BEST SELLER!

Created By Lucid
Solutions Inspiring Confidence

Anyone who has given birth to an Exchange network knows it can get sick and needs some nursing to stay healthy. In fact, 72% of Exchange Administrators surveyed* have "experienced" an Exchange disaster (feels like the flu)—usually from improper feeding and care.

Like many databases, constant adding and deleting can corrupt an Exchange data file so it eventually turns sour. Replicating, archiving and backing up the data doesn't stop the stink—it just stores it. You've got to…

Fix the Problem

You may have tried the free utilities to fix Exchange. While they help, they are too tedious, time consuming and lightweight to keep your Exchange baby healthy. You've tried the milk, now try some meat!

Pamper Yourself with GOexchange

It's time to try GOexchange, from Lucid8, the #1 best-selling automated disaster prevention and optimization software for Microsoft Exchange 5.5, 2000, 2003 and 2007. As the mother of all Exchange tools, GOexchange helps prevent disasters, repair problems, improves performance, and saves you a lot of time.

> ***"Without routine maintenance, decreasing performance, increased warnings and errors accumulate and database fragmentation transpires, leading to Exchange disasters."***
>
> Gartner

Prevent Hiccups

GOexchange removes errors, warnings and inconsistencies within the database—before major corruption makes the database fail.

> ***"GOexchange corrected 2,264 errors and 26 warnings."***
>
> Paul Ramos, Director IT

Run, Don't Crawl

In addition to fixing the database, GOexchange removes sluggishness and improves performance by re-indexing and defragmenting the database to permanently remove white space and deleted items. The end result is increased performance and stability with a compact efficient database that's 31 to 55% smaller! Combine this with archiving and the database is up to 91% smaller—making it much quicker to backup.

> ***"..our information stores were reduced by 45-50%."***
>
> Dale Huitt, Systems Lead

Automated Babysitter

First, GOexchange is easy to setup and use. Twenty minutes—that's all it takes to get your server up and running. Just schedule it, and walk away!

The software notifies the users, validates the database, runs the backup, conducts a comprehensive system analysis and diagnostics, logs the errors, and notifies you if it discovers a "stop" error—then it repairs and defragments the database, generates a thorough report and schedules the next event.

You can do some of this work yourself, but why waste time doing repetitive maintenance, when GOexchange can do it for you—faster and more effectively than doing it by hand.

> ***"Life before GOexchange…was an absolute nightmare, late nights, long weekends and upset users."***
>
> Marty Grogan, CTO

Stop The Crying

Why not call now, or visit our resource site and learn how to reduce the risk, and avoid the pain. Protect your exchange data, maximize performance, and spend a weekend at home—*instead of babysitting Exchange.*

Special Offer

- Free Software for analysis of your Exchange server!
- Free White Paper—"Basic Feeding of Your Exchange Server."
- View the Gartner webcast: "Protecting Microsoft Exchange…"

Go to: www.Lucid8.com/GoITPro
Call 425.456.8474
E-mail: Sales@Lucid8.com

Meet Email-Retention Needs with Exchange 2007

Use messaging records management and transport rules to achieve compliance

by Brien Posey

(http://www.brienposey.com) is the vice president of research and development for Relevant Technologies. He also writes technical content for a variety of publications and Web sites.

Over the last several years, many laws have been passed that set specific requirements for email retention. Although various third-party products such as AdvisorMail, Optiva Systems's ArcMail E-Mail Defender, and Quest Software's Quest Archive Manager can help organizations running Microsoft Exchange Server 2003 comply with these regulations, Exchange 2003 wasn't designed with long-term mail retention in mind. Not surprisingly, Exchange Server 2007 addresses these shortcomings. Although Exchange 2007 probably won't be completely compliant with federal regulations such as the Sarbanes-Oxley (SOX) Act right out of the box, it offers mechanisms that make achieving compliance easier.

This article was written in November 2006. As such, information that I discuss here is based on a beta version of Exchange 2007 and could potentially change by the time the final product is released. However, Microsoft is far enough into the beta cycle that I don't anticipate any major changes to the way that Exchange 2007 works.

Messaging Records Management

When you hear people discuss making a mail server compliant with the latest regulations, one central theme that usually comes up is message archiving. Various laws require email to be retained for specific lengths of time. But you can't depend on users to save a copy of every message. Even if users consistently saved all their mail, locating specific messages on demand would be nearly impossible because the messages would be scattered among the users' mailboxes.

An Exchange 2007 feature that can help make message archiving easier and more reliable is messaging records management, which lets you assign retention rules to specific folders. When used in conjunction with transport rules, messaging records management can sort and archive messages according to your company's needs.

To demonstrate how messaging records management works, suppose that you want to keep users' mailboxes clean by implementing an email-retention policy mandating that any message more than three months old be deleted. Let's also suppose that you're required to keep any messages related to the Contoso account for five years.

In a situation like this, you could create a managed custom folder with a five-year retention period. You could then create a mailbox that's used solely as a repository for messages related to the Contoso account. Because this mailbox has a special purpose, you wouldn't apply your regular retention policy to it. Instead, you'd create a transport rule that captures any message mentioning the Contoso account and sends a copy of the message to the designated mailbox. Then you'd use a Microsoft Office Outlook rule to move messages arriving in the mailbox to the managed custom folder with the five-year retention period.

If you're used to running Exchange 2003, this method probably seems completely foreign to you. But the technique sounds more difficult than it really is. For an outline of the procedure, see the sidebar "Step-by-Step Email Retention in Exchange 2007" on page 48. Now, let's look more closely at how to implement it.

Create a Managed Custom Folder

The first step in this technique is to create a managed custom folder and assign a five-year retention period to it. To do so, open Exchange Management Console (formerly known as Exchange System Manager) and expand the Organization Configuration container, then select the Mailbox container beneath it. The console's middle pane displays a series of tabs related to the Mailbox container. Select the Managed Custom Folders tab, then right-click in the empty area beneath it. Choose the New Managed Custom Folder command from the resulting shortcut menu to launch the New Managed Custom Folder wizard. (Managed folders are available organization-wide, so you can apply them to any mailbox throughout the organization.)

As you can see in Figure 1, page 46, you start by entering a name for the new folder. For this scenario, enter Contoso Account as the folder name. As you enter the name, the text box below it automatically fills in the name that users will see when they view the folder in Outlook. You can enter additional text in the large text box so that it's displayed when users view the folder through Outlook. For this example, enter the following text: *All messages related to the Contoso account must be retained for five years.* Finally, select the *Do not allow users to minimize this comment in Outlook* check box. (Note that only Microsoft Office Outlook 2007 and Microsoft Outlook Web Access—OWA—2007 display this check box.)

Click the New button to finish creating the folder. Exchange displays a summary of the action along

with the Exchange Management Shell command that you can use to script the action in the future. Click Finish to close the wizard.

Now that you've created the new managed folder, it's time to configure a retention policy for it. The Contoso Account folder now appears in the Mailbox container, as Figure 2 shows. To configure the folder's policy, select the folder, then click the New Managed Content Settings link in the Contoso Account pane on the right side of the screen.

At this point, the New Managed Content Settings wizard opens, as Figure 3 shows. Begin by entering a descriptive name for the new settings. Set the *Message type* option to All Mailbox Content, then select the *Retention period (days)* check box. Because we're retaining messages for five years, enter 1827 (365 days × 5 years + 2 days for leap years). Set the retention period to start when an item is moved into the folder, then set the items to be permanently deleted when the retention period expires, as I've done in Figure 3. A permanent delete removes the item from the database, so users won't be able to use the Recover Deleted Items feature to retrieve items from the dumpster.

Click Next, and you'll see a screen explaining that journaling can be used to automatically forward a copy of an item to an alternate location. You might want to investigate using the journaling option in other scenarios, but for this example click Next to skip it, and you'll see a screen displaying a summary of the configuration settings you're implementing. Click New to create the settings. When the process is completed, click Finish.

Figure 1: Creating a managed custom folder

Figure 2: Contoso Account folder in the Mailbox container

Figure 3: Configuring a managed-folder retention policy

Set a Mailbox Retention Policy

So far we've created a folder for the Contoso account and set a retention policy for it. As you'll recall, though, our other goal was to keep user mailboxes cleaned out by preventing messages from being stored for more than three months. To do so, we'll create a mailbox retention policy that's similar to the one we created for the Contoso Account folder.

Navigate through the Exchange Management Console tree to the Organization Configuration\Mailbox container. When you select the Mailbox container, the details pane displays a series of tabs. Select the Managed Default Folders tab to display a list of all the default mailbox folders.

Right-click the Inbox folder, and select New Managed Content Settings from the shortcut menu to launch the New Managed Content Settings wizard. As before, you'll enter a name for the new setting. Let's call this policy *Three-Month Retention*.

For this article, set the message type to All Mailbox Content. For other policy scenarios, you could segregate messages by categories such as documents, calendar items, meeting requests, voicemail, and so forth. Now select the *Retention period (days)* check box, and set the retention period to 90 days. Configure the retention period so that it begins when an item is delivered to the mailbox. Set the end-of-retention-period action to move expired items to the Deleted Items folder.

Click Next, and you'll see the Journaling screen. For the purposes of this example, we're not interested in journaling copies of every message, so click Next. You'll see a summary of the new managed-content settings. Assuming that all the information is correct, click New to create the new policy. When the process is completed, click Finish. (Note that you could also apply this policy to the Sent Items folder.)

Create a Managed-Folder Mailbox Policy

Although we've set a retention period for the Inbox, we still have to create a policy that references this retention period. The policy lets you group together multiple managed folders in a single step.

To create this policy, navigate through the

console tree to Organization Configuration\Mailbox. Select the Mailbox container, and click the Managed Folder Mailbox Policies tab in the details pane. Next, right-click in an empty area of the details pane and select the New Managed Folder Mailbox Policy command from the shortcut menu. When you do, Exchange launches the New Managed Folder Mailbox Policy wizard.

Once again, start by entering a name for the policy. For this scenario, call the policy Managed Folders. Now, click Add to reveal a list of available folders. Choose Inbox from the list and click OK, then New, then Finish.

At this point, repeat the procedure to create a second managed-folder mailbox policy. Let's call this one Contoso. You'll do everything the same as before except that rather than associating the policy with the Inbox, you'll associate it with the Contoso Account folder that you created earlier.

Associate the Policy with Mailboxes

You've created a policy that you can associate with the user's mailboxes to effectively place a three-month maximum retention period on mailbox items. To add the policy to a mailbox, navigate through the console tree to Recipient Configuration\Mailbox. The details pane displays a list of available mailboxes. Right-click the mailbox you want the policy applied to, and select the Properties command from the shortcut menu. Exchange displays the mailbox's properties sheet.

Select the properties sheet's Mailbox Settings tab, then select the *Messaging Records Management* option and click the Properties button. You should now see the Messaging Records Management dialog box that Figure 4 shows.

Select the *Managed folder mailbox policy* check box, then click Browse. You should see the policy created in the last step (we called it Managed Folders). Select this policy and click OK three times to close all open dialog boxes. The policy is now associated with the user account and should be active at this point.

Create a Transport Rule

The next step in the process is to create a mailbox that can act as a repository for messages related to the Contoso account. Create this mailbox in the typical way. Go through the steps to associate a managed-folder mailbox policy with the new mailbox, and choose the Contoso policy.

Now that you've created a mailbox to act as a message repository, the next step is to move Contoso messages into the mailbox. The easiest way to accomplish this is to create a transport rule. Transport rules look at messages as they flow through the Exchange organization.

To create a transport rule, navigate through the console tree to Organization Configuration\Hub Transport. Next, click the New Transport Rule link in the Actions pane to launch the New Transport Rule wizard.

The wizard's initial screen asks you to enter a name for the rule as well as an optional comment. Let's name the rule Contoso, and we'll add a comment indicating that the rule copies Contoso-related messages to a repository mailbox.

Click Next, and you'll see a screen asking you to select a condition for the rule to look for. There are many conditions that you can specify, but let's assume that a message will be considered to be related to the Contoso account if the word *Contoso* appears anywhere in the message subject or body. Therefore, select the *when the Subject field or the body of the message contains specific words* check box, as Figure 5, shows.

Notice in Figure 5 that *specific words* is underlined in the edit section in the bottom pane. Click the *specific words* link to enter the words you want the rule to apply to. In this case, just enter Contoso.

Click Next, and you'll be prompted to select an action for the rule. In this case, choose the *Blind Carbon Copy (BCC) the Message to Address* option. Doing so will cause a copy of every message containing the word *Contoso* to be sent to the repository mailbox. Just as you clicked the *specific words* link earlier, you must now click the Address link to enter the email address that's associated with your repository mailbox.

To complete the process, click Next twice, followed by New and Finish. The new transport rule is now created.

Create an Outlook Rule

We're almost done except for one minor detail. The Inbox associated with the repository mailbox that we created doesn't have a message-retention policy associated with it. We need to guarantee that Contoso-related messages are retained for five years. We've created a managed custom folder that has a five-year retention period associated with it, though, so we just need to move messages from the Inbox folder to our managed custom folder.

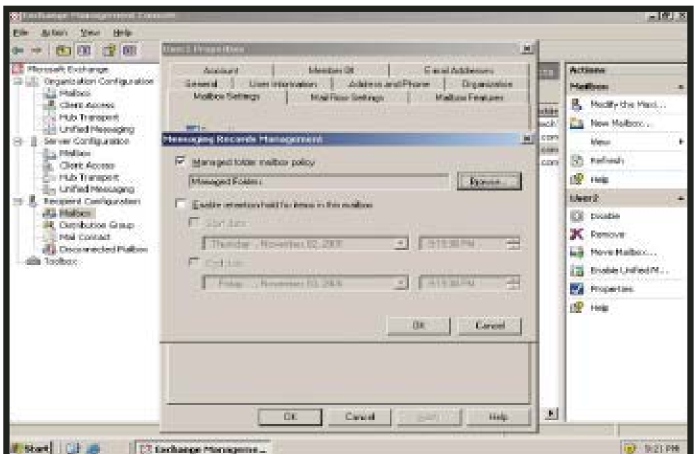


Figure 4: Associating a retention policy with user mailboxes

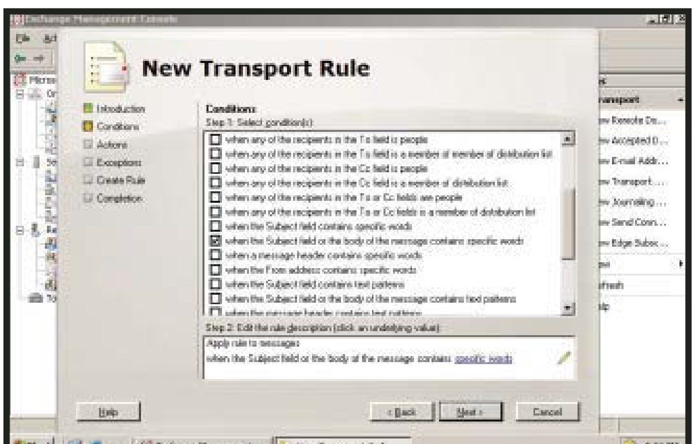


Figure 5: Selecting the condition for a transport rule

STEP-BY-STEP EMAIL RETENTION FOR EXCHANGE 2007

Exchange Server 2007 has the tools to help you achieve email-retention compliance both with current legislation and your company's particular needs. These steps outline the procedure to limit Inbox items to three-month retention while holding all messages related to a specific account for five years.

STEP 1: Create a Folder with a 5-Year Retention Period

Use Exchange Management Console to launch the New Managed Custom Folder wizard. Create the managed custom folder for your specific account, then use the New Managed Content Settings wizard to configure a five-year retention policy for the folder.

STEP 2: Set a Mailbox Retention Policy

Use the New Managed Content Settings wizard to set a three-month retention policy for user mailboxes.

STEP 3: Create a Managed-Folder Mailbox Policy

Use the New Managed Folder Mailbox Policy wizard to reference the retention period for the Inbox. Repeat this step to create a second managed-folder mailbox policy and associate it with the managed custom folder.

STEP 4: Associate the Policy with Mailboxes

Associate the retention policy with a particular mailbox through the mailbox properties sheet's Mailbox Settings tab.

STEP 5: Create a Transport Rule

Create a repository mailbox for messages relating to your specific account, then use the New Transport Rule wizard to create a rule that moves messages relating to the specific account into the repository mailbox.

STEP 6: Move Necessary Items to the Managed Folder

Use an Outlook rule to move items relating to the specific account from the repository mailbox's Inbox to the managed folder with the five-year retention policy.

InstantDoc ID 94739

Unfortunately, you can't do so through Exchange Management Console, but you can get the job done through Outlook by creating an Outlook rule. The procedure I'll describe is designed for use with Microsoft Office Outlook 2007.

Open the repository mailbox in Outlook, then choose Rules and Alerts from Outlook's Tools menu. When the Rules and Alerts dialog box appears, click the New Rule button. Outlook displays various rule templates. Click the *Check Messages When they Arrive* option found in the *Start from a Blank Rule* section, then click Next.

You'll see a screen displaying various rule conditions. Select the *Where my name is not in the To box* check box. Remember that our transport rule sends messages to this mailbox by using a BCC, so the mailbox owner's name should never appear in the To box.

Click Next, then select the *Move it to the Specified Folder* check box. Click Specified, and you'll see a list of folders. Select the folder to which the retention policy applies, then click Finish, followed by OK.

Achieve Your Compliance Goal

As you can see, configuring Exchange 2007 to retain specific types of messages can be a lot of work. Nevertheless, doing so is usually worth the effort because messages required to be retained will all be grouped into a central folder that you can easily search for specific information. Messaging records management combined with transport rules will help you meet your organization's email-retention needs.

InstantDoc ID 94607

Disaster-Preparedness Checklist

5 steps to putting a disaster-recovery plan in place now

What would happen to your business if a disaster were to strike? What would happen if your business were shut down for a day? For a week? For a month? At some point, if you can't do business, you'll be out of business. You can't always prevent disasters, but having a disaster-recovery plan (DRP) can prevent a disaster from ruining your business.

Also known as a business continuity plan, a DRP outlines the steps that need to be taken if an event occurs that stops your business sites from operating. The DRP helps your business continue to function.

Preparing your company to survive a shutdown isn't simple, but careful planning coupled with follow-through can turn a potentially business-ending event into a temporary interruption. The Gartner Group has said that 40 percent of business enterprises that experience disaster go out of business within five years of the event. If you want to be in the 60 percent of businesses that survive, you must have a DRP in place before a disaster and follow the plan if a disaster occurs. (Gartner has done many reports on disaster preparedness, which you can find at http://www.gartner.com/1_researchanalysis/focus/aftermath.html.)

The complexity of your disaster preparations depends on several factors, including the size of your business. In most cases, recovering a small business is easier than recovering a large business. But although a large business might require a more extensive or complex plan than a small business, all disaster-planning processes, regardless of the size of the business, should include the steps outlined in the sidebar "Disaster-Recovery Checklist," page 52.

A complete recovery plan includes technical, personnel, and facilities considerations. I walk through the IT aspects here, but remember, your plan must also adequately address crucial facilities and personnel requirements.

Put Together Your DRP Team

The first step in creating a DRP is putting together the planning team, typically a management team that determines what needs to be in the DRP and designates who's responsible for each part of the plan. In a small business, the DRP team might simply be the company owner and the IT person. In a large corporation, the DRP team might be made up of the department heads or division vice presidents. In all businesses, the DRP team needs to include people who are empowered to make key decisions and who know what data and business processes need to be protected in the event of a crisis.

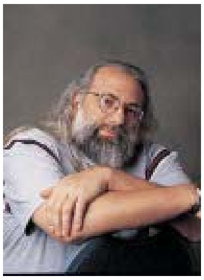
In your DRP, you need to address budgetary, organizational, and business-process requirements, and the DRP team must agree on how to handle these requirements. The DRP team can delegate some responsibilities—for example, the team might assign certain steps to subordinates whose expertise covers what needs to be done—but it's crucial that DRP team members have authority to make the decisions necessary to implement the complete plan.

Evaluate Your Business Processes

After you have the DRP team in place, it's time to evaluate your business processes and determine which business functions are "mission critical," which are "must-haves," which are "nice to have," and those that aren't essential. First, identify which business processes are needed for the business to continue in a crisis. Then, determine the minimal technology resources that your business needs to restore those processes. Note that although disaster recovery is often expensive, even in a small company, when the DRP team determines the minimum requirements, you must be prepared to preserve resources and not cut any resources below that minimum level. There's little point to having a DRP that requires redundant hardware and software systems if someone up the corporate chain of command decides that sufficient money or support isn't available for those resources.

When determining what equipment is needed for the recovery plan, you'll want to point out the investments that serve double duty. For example, you might determine that you need to have network servers in reserve, but you can't do much with that hardware while it waits to be used; if you put reserve servers into service, you increase the number of systems for which you need to provide redundant hardware. But you can maximize your investment. Although hardware such as online and offline data-protection systems are crucial to your DRP, you can also make them everyday parts of your IT process. Your recovery plan might, in this case, motivate the business to add additional capabilities and features beyond what you need for regular backup and recovery so that the expenditure towards the DRP is incremental. For example, you might add new generations of backup and recovery hardware, which improves day-to-day workflow and improves your disaster preparedness.

The DRP team also needs to decide what level of catastrophe the business is prepared to recover from. Your DRP might cover everything from a simple short-term telephony or networking outage to a full-blown Hurricane Katrina–level devastation of local public and private infrastructure. However, most plans commonly focus on catastrophes that are the most likely (fire, flood, weather problems). Be sure to specify the level of disaster your DRP addresses.



David Chernicoff
(david@windowsitpro.com) has been writing computer-related features and product reviews for more than 15 years and is coauthor of *Microsoft Windows XP Power Toolkit* (Microsoft Press).

Detail the IT Aspects of Disaster Recovery

In "Backup and Recovery Basics" (January 2007, InstantDoc ID 94307), we talked about your *data backup and recovery plan*. You'll want to include that data plan in your DRP. The data-recovery plan should, at a minimum, cover the basics of protecting your mission-critical (and valuable) corporate data. Note that some items that are optional in simple data-backup plans may become requirements in DRPs. For example, your backup and recovery plan will likely include the ability to restore servers if they crash. Perhaps you've even provided backup server hardware. But as part of a good DRP, you might want the ability to restore servers to non-identical hardware, which would then require extra steps in the backup and restore process.

If your business is large enough, your DRP might include a plan for duplicate data centers, set up as redundant sites. If your business is large enough to have multiple data centers, you might want extra capability at each site to intervene should a data center become unavailable. In all cases, you need to be able to back up data offsite so that the loss of the primary location doesn't mean the end of your business.

Offsite data storage can range from the low end (an employee is responsible for taking the daily backup tapes to a secure offsite location) to the high end (sufficient network bandwidth is available to allow for real-time data replication to offsite storage). Internet-based backup and recovery systems can serve a dual purpose, providing regular backup and recovery services along with a reliable and secure offsite location for mission-critical corporate data.

Test and Implement the Disaster-Recovery Plan

You've decided what aspects of your business to protect and how you're going to protect them. Now you're ready to test and implement the DRP. This means documenting each DRP task, outlining the order in which the tasks should be carried out, designating the person responsible for seeing each task is completed, specifying who manages the entire DRP operation, and testing the entire DRP.

After you roll out any additional hardware or software, you'll want to walk through the entire DRP, making sure that the planning documentation matches the actual recovery process. This is the time to make necessary changes to the plan or to the technology. Remember, as you make changes, you'll want to re-confirm previous

ULTRABAC SOFTWARE

USERS OF: TSM | MS VIRTUAL SERVER | SAN | WINDOWS | FTP | VMWARE

These People Are Jumping For Joy Because:

a. They are using a Windows-based Bare Metal Recovery (BMR) product that can also be 100% integrated with IBM's Tivoli Storage Manager.

b. They are leveraging their disaster recovery investment using TSM, NAS/SAN, network, tape, library, FTP, etc.

c. They have true dissimilar hardware restore capability.

d. They can perform virtual-based disaster recoveries using VMware or MS Virtual Server 2005.

e. They can use IBM Global Services (or any other service for that matter) to easily recover critical Windows servers that have been physically destroyed.

f. They can fully recover a failed server to 100% operational status in 15 minutes or less.

g. **All of the above. They discovered UBDR Gold bare metal disaster recovery.**

Answer: If you answered **g**, then you are also in the know: UBDR Gold is the only disaster recovery product on the market that provides all of these options and more (if you didn't choose g, download your free demo today). UltraBac Software has been consistently recognized as being first to market with many critically acclaimed Windows-based backup and disaster recovery innovations. UBDR Gold is our finest example–consistently being at the forefront of features for bare metal restore. With 24 years of experience and over 100,000 servers being protected in organizations around the globe, we know what it takes to create happy customers. We provide reliable software, strategic product functionality, competitive pricing, and a hard-to-come-by level of technical support customers expect and deserve.

BACKUP AND DISASTER RECOVERY SOFTWARE FOR PEOPLE WHO MEAN BUSINESS > WWW.ULTRABAC.COM

steps to make sure that they still apply. Having a DRP is not a one-time event: You need to keep working through the DRP until you achieve repeatable, consistent results.

When you're certain that the DRP works and that the documentation accurately reflects the process, you're ready to have the DRP team approve the final version of the DRP. Then, you're ready to distribute the plan as appropriate, in whole or in part, to all affected parties. Also, be sure you have secure offsite storage for printed copies of the detailed DRP.

The Ongoing DRP Process

Even though you now have a DRP in place, you've only just begun the disaster-recovery process. Very few businesses are static, so as business changes, your DRP will also change. As with any business-critical activity, testing and maintaining your DRP is an ongoing process. As you add technology to your business, you must determine how the new technology affects the DRP, then change the DRP and associated processes as necessary. Changes in the way you do business can also affect the DRP, so be sure that you alter the DRP to reflect any changes to business workflow. Regularly evaluate your plan—how often you evaluate depends on how fast and how often the business changes. Simply documenting changes is unlikely to be sufficient. Your DRP should be tightly integrated into your business model—any changes to the business also mean that the DRP will change and need to be updated and re-tested.

The job of the DRP planning team continues as well. The composition of the team may change somewhat after a functional DRP is in place, but the DRP team still needs to organize the management and maintenance of the DRP. Regularly scheduled DRP team meetings can give multiple departments the chance to interact and the opportunity to provide recommendations for current and future updates of the DRP and its processes. Continuing involvement with the DRP team also helps remind business staff of the ongoing importance of having an up-to-date disaster-recovery plan.

Various analysts studying disaster recovery have noted that nearly 50 percent of all large companies lack any sort of comprehensive DRP, with that number climbing closer to 80 percent when small businesses are included in the calculation (for more information, see http://www.gartner.com/1_researchanalysis/focus/aftermath.html). Every business, regardless of size, can benefit from having a DRP. Defining what needs to happen in the event of an emergency lets you gain some control over a crisis that might otherwise put you out of business. Implementing a DRP, even on a small scale, can make the difference between business survival and failure.

InstantDoc ID 94564

DISASTER-RECOVERY CHECKLIST

Will you be ready if disaster strikes? Follow these steps to be sure you're prepared.

☐ STEP 1: Create a Disaster Recovery Plan (DRP) Planning Team

- Choose team members who have decision-making approval and sufficient authority to gather information companywide.
- Define team members' responsibilities.
- Create a clear organizational chart that outlines who is responsible for each aspect of disaster-recovery planning.

☐ STEP 2: Evaluate Your Business Processes

- Evaluate and rank (in order of importance) all business processes.
- Define what business processes, technology, systems, and applications must be restored for the business to continue operating.
- Determine the level of disaster protection you want to achieve.

☐ STEP 3: Determine Which IT Processes Will Be Incorporated into the DRP

- Evaluate existing backup and recovery processes.
- Integrate existing processes into the DRP.
- Upgrade existing processes as necessary.

☐ STEP 4: Implement and Test the DRP

- Document all duties and responsibilities of people who have disaster-recovery roles.
- Roll out any additional hardware or software needed.
- Test the DRP by walking through the disaster-recovery process.
- Based on feedback from the walk-through, modify the DRP to reflect the actual process.
- Get final management approval before distributing the final DRP documents.
- Distribute the final DRP documents to all involved parties.
- Maintain and securely store offsite printed copies of all DRP documentation.

☐ STEP 5: Maintain an Ongoing DRP Process

- Schedule regular DRP team meetings so that different departments can interact and provide ongoing input into keeping the DRP relevant and up-to-date.
- Carry out regularly scheduled DRP tests.
- Schedule regular updates to the DRP to accommodate changes to business processes or technology infrastructure.
- Schedule regular evaluations of technology and workflow, and update the DRP accordingly.
- Assign responsibility for all DRP update and maintenance programs to key people, plus designate a central person or persons who'll be responsible for cross-checking any changes.

InstantDoc ID 94565

Perimeter Security

You need a multilayer solution to keep your systems safe

You probably remember the "old days," when setting up security commonly meant using a firewall. But even then, this was a woefully narrow viewpoint. Establishing perimeter security requires much more than using firewalls and detecting intrusions. A firewall is only one component of perimeter security, and perimeter security is just one component of security. Here are some things to consider when establishing perimeter security and a checklist (page 42) you can use to plan perimeter security in today's environment of increasing connectedness.

Beyond Firewalls

Perimeter security still begins with the venerable firewall. People often (wrongly) assume that a firewall scrutinizes every inbound packet. Firewalls are only a first line of defense, and they prevent only the most elementary attacks. Simply put, firewalls evaluate packets according to the message-access protocol and the state of the connection between the internal and external computer. If the packet matches a protocol allowed for incoming connections, or if the packet is part of an established outbound connection, the firewall allows it to pass. Any malicious content inside an allowed-protocol or outbound-initiated connection will pass through a firewall undetected. For example, if you have a mail server behind your firewall, you'll probably open up port 25 (SMTP) on your firewall for incoming connections and redirect such connections to your mail server. As soon as the firewall identifies that a packet is SMTP, it forwards the packet to the mail server.

Any firewall you buy today will include the two main features of a modern firewall: *stateful packet inspection* and *network address translation (NAT)*. With stateful packet inspection, the firewall is intelligent about and attentive to connection-oriented protocols such as TCP, preventing attackers from sneaking malicious packets past the firewall by posing as an already-established connection. NAT conceals details about the internal network, such as the internal LAN's addresses and topology, by replacing the internal network address and port with its own Internet address and a new port number.

Application Gateways

Every protocol and application is vulnerable to malformed data and irregularities inadvertently introduced by the designers and coders of the associated software. More and more applications are exposed to potentially hostile computers and malicious content or traffic on the Internet that can contain bad data. And the risk increases with the drive toward greater mobility. To provide a more transparent experience for mobile users, common practice is shifting away from virtual private networks (VPNs) to secure remote access at the application level. For example, Microsoft Exchange 2003's support for remote procedure calls (RPC) over HTTP allows users to use Outlook inside or outside the LAN with no difference in the user experience. And more and more companies are integrating processes with their business partners at the transaction level by using Simple Object Access Protocol (SOAP) and related protocols. As a result, organizations are exposing a larger attack surface at the application level, and hackers are taking advantage and delivering application-level attacks.

You can lower the risk of these higher-level application-specific attacks. To do so, you must first keep all applications that communicate with potentially untrusted external systems fully up to date. Proactively installing all patches to OSs and applications is key to ensuring perimeter security. (Keep in mind that patching can be undermined by newly discovered vulnerabilities being made public before a patch is available.)

You can take a more proactive approach to application-level network attacks by using an application-level gateway (also known as a *reverse proxy*). Application-level gateways can look for specific known attack methods, but that's not their focus. An application-level gateway inserts a system between the Internet and the application server that understands the relevant application protocol that's in use. This application-level gateway's system appears to the outside world as the end-point application server, but in actuality, the gateway interprets each incoming request, reduces the request to the application server's own internal lexicon, then builds a new request from scratch discard or prevent any malicious, malformed content from getting through. The gateway then sends the new request to the actual application server and processes the server's reply in a similar way. For example, an SMTP gateway that carefully deconstructs an incoming SMTP message and then rebuilds it from scratch with strict adherence to the SMTP protocol specification discards any malformations such as invalid character sequences or buffer overflows in the message.

Organizations have differing application gateway needs, but almost all use applications and protocols for Web browsing (via HTTP), email (via SMTP), and instant messaging (IM). These three protocols make applications particularly attractive targets to four types of attacks: direct attacks, malware infection, phishing, and outbound content risks. Direct attacks that use buffer overflow or other vulnerabilities specifically target weaknesses in email clients and servers, Web servers, and IM

by Randy Franklin Smith

(rsmith@ultimatewindowssecurity.com) is a contributing editor for *Windows IT Pro*, an information security consultant, and CEO of Monterey Technology Group. He teaches Monterey Technology Group's Ultimate Windows Security course series and is an SSCP, a CISA, and a Security MVP.

clients. Because HTTP, SMTP, and IM all support file transfers, all three are particularly vulnerable to malware infection. These same protocols also allow social engineering attacks such as phishing. The risks associated with these protocols aren't limited to inbound content—outbound content (email messages, Web postings, and instant messages) sent from employees can expose organizations to risks that endanger privacy, confidentiality, and regulatory compliance.

Although no product on the market provides application-level gateway support for every protocol and application, Microsoft's ISA Server offers the widest native support (including for SMTP, HTTP, FTP, and RPC). ISA Server also supports a variety of partner-developed plug-ins for other protocols and applications. ISA Server's extensible architecture and Microsoft's successful collaboration with partners help position ISA Server as a type of universal application gateway, but you can also use some of the many best-of-breed solutions for specific applications (e.g., FaceTime's solutions for IM security and antispyware). Web-filtering solutions, such as those from Barracuda Networks, Websense, St. Bernard Software, and SurfControl, help you enforce policies that determine where internal users can go on the Web. By using keyword monitoring, such solutions also help you monitor employees or block them from sharing confidential information or posting or accessing inappropriate content.

Beyond Web, email, and IM vulnerabilities, application-level perimeter risks also come from peer-to-peer (P2P) networks, Web conferencing, and XML. Many developers of application-gateway solutions originally designed for Web filtering and IM security are extending their solutions to support P2P and Web conferencing.

The growing use of XML communications, especially in the form of SOAP, for business transactions poses problems different from those of the more end-user–based technologies I've been discussing. IT uses XML to link mission-critical business systems with business partners' corresponding systems. The text-based nature of XML makes any security solution rely heavily on CPU and memory resources because of the recursive parsing involved. Administrators are understandably loathe to put an added load on application servers, and the number of application servers affected can quickly grow out of control in organizations that use XML. If your organization uses XML, you'll want to add an appliance-based XML firewall to your array of perimeter defenses. (For more information, see Market Watch: "SOAP/XML Firewalls," September 2003, InstantDoc ID 39755.) Solutions are available from DataPower, Xtradyne, Reactivity, and Layer7 Technologies.

One of the worst mistakes you can make with perimeter security is to issue policies that forbid using certain technologies such as IM or Web conferencing. Users will ignore such policies, and service providers and developers will find a way around simple firewall rules designed to block "unauthorized" communications. Don't risk compromising your role and effectiveness as an IT professional by hindering rather than facilitating technology use. As you address security issues, facilitate adoption of new technology.

VPNs and SSL VPNs

Despite the trend toward providing remote access at the application level, VPN access is still very important to mobile and remote users. VPNs have become confusing with the advent of so-called Secure Socket Layer (SSL) VPNs. Let's talk about traditional VPNs, then I'll define SSL VPNs and discuss their pros and cons.

Traditionally, using VPNs for remote access simply meant establishing a connection over the Internet to the company LAN by using a tunneling protocol such as PPTP or L2TP. Once connected, remote users were virtual members of the internal LAN and could access IP-accessible resources on that LAN as if they were in the office (although access was much slower due to the latency of the remote connection).

True PPTP- or IPsec-based VPNs have an undeserved reputation as hard to administer and support (the biggest complaint is that you must install proprietary client software on all remote users' PCs). I don't understand why companies have relied so much on third-party VPN solutions rather than on the native Windows PPTP and L2TP support. Installing an RRAS server is easy, and Windows has had a built-in VPN client since Windows NT. Using PPTP is especially easy. If you want two-factor authentication using client certificates, you'll have to use L2TP and deploy client certificates (but that's true with any type of two-factor authentication). Using the Connection Manager Administration Kit (CMAK), you can create a wizard that automatically sets up the

PERIMETER SECURITY CHECKLIST

Use this checklist to plan your perimeter security solution.

- [ ] Identify all physical and logical connections to the outside world.
- [ ] Take the lead in implementing new Internet-based technologies securely from the start.
- [ ] Protect all routes through which files can enter your network with anti-malware software.
- [ ] Always patch all OSs, perimeter-related devices, applications, and servers as soon as patches are available.
- [ ] Insulate remotely accessible applications with application-level gateways such as ISA Server and plug-ins from ISA Server partners.
- [ ] Consider advanced perimeter security solutions for IM, XML, and Web filtering.
- [ ] If you need an IDS or IPS, plan for the necessary support and maintenance.

InstantDoc ID 94855

VPN connection in the user's Network Connections folder. You can distribute the wizard as an email attachment, on a CD-ROM, or as a Web download.

The biggest problem I've encountered with VPNs is caused by firewalls between the VPN server and the remote user. Most firewalls must be explicitly configured to allow PPTP or IPsec (L2TP rides inside of IPsec) pass-through for outgoing VPN connections, and not all administrators are willing to do this. These occasional connectivity problems are one of the reasons to use SSL VPNs instead.

Not all SSL VPNs are true VPNs—many are simply a reverse HTTP Secure (HTTPS) proxy. With a reverse proxy server, you can take browser-based applications originally deployed for access by internal LAN users and make them available to remote users without changing the internal application server. The proxy server poses as a secure Web server on the Internet; after remote users successfully connect and are authenticated using their normal Web browsers, the proxy server acts as middleman between the user and intranet server. ISA Server has been doing this for many years, but the term "SSL VPN" has come into use as new companies have gotten in on the reverse proxy game. The key advantage to using a reverse proxy is that you can easily make internal Web applications available to remote users without doing any client-side setup or installation and without modifying the internal Web application. And you don't run into the connectivity problems I mentioned earlier caused by firewalls blocking outgoing tunneling protocols.

Use a reverse proxy when you need to provide remote access to an internal Web application. Use SSL VPNs when you need remote network access to the internal network at the transport level (TCP/UDP). True SSL VPNs provide tunneling of IP traffic between the internal LAN and the remote user. OpenVPN is an open-source, true SSL VPN. For more information, read "Putting OpenVPN to Work" (May 2005, InstantDoc ID 45844). Other true SSL VPNs are available from ISVs such as Aventail and Citrix. SSL VPNs make a lot promises as to ease of use and administration and lower cost of ownership, but Windows native VPN options work well if you use the management capabilities of CMAK, Group Policy, and Certificate Services. If you must support non-Windows remote users, SSL VPNs can be a more compelling option. For an informative guide to SSL VPN products, see Buyer's Guide: "SSL VPN Products" (April 2005, InstantDoc ID 45612).

Intrusion Detection

Despite your best efforts to deploy an array of perimeter security defenses, there's still the risk that attackers can penetrate your network, so you'll want to think about intrusion detection and prevention. Intrusion detection systems (IDSs) and intrusion prevention systems (IPSs) use one or more of three basic technologies to detect intruders: packet examination, policy configuration, and pattern analysis. Most IDS and IPS solutions examine packets for known attack signatures. The effectiveness of this detection method depends on how many attack signatures the vendor builds into the product and how often it's updated. Most systems also let you configure policies that define expected network traffic patterns, but this method requires a lot of research and work, and you must maintain the policies as new applications are brought on line and traffic patterns change. Some systems employ various algorithms and pattern analysis in an attempt to automatically detect anomalous traffic. These systems hold promise for the future, but right now they suffer from the same limitations and false positives as do heuristics- and Bayesian analysis–based antispam solutions.

IDS and IPS solutions don't vary as much in detection features as they do in the ways they respond when they detect suspicious or unauthorized traffic. IDS solutions focus on logging and alerting. IPS solutions attempt to stop the intrusion by reconfiguring the firewall in real time or by issuing TCP resets. When IDS solutions get it wrong (return false positives), your Inbox fills up and your pager melts down from too many alerts. When IPS solutions get it wrong, important business processes are stopped dead in their tracks. Unless you can dedicate staff to an IDS or IPS, your resources might be better spent on direct perimeter security solutions.

Perimeter security used to be a matter of configuring firewall rules; now, perimeter security is a multifaceted, multilayered, and much more complicated area of security, and it's much more than the boundary between the Internet and your intranet. Today, many applications straddle these two networks through logical connections that essentially circumvent your firewall. The first step in planning perimeter security is to identify all your connections, both physical and logical, to the outside world. It's important to remember that perimeter security changes constantly and additional perimeter connections crop up as new technologies to leverage the Internet are created. For example, remote-control–based services, such as GotoMyPC, are quickly gaining momentum. Users can easily subscribe to and use GotoMyPC for remote access, but when they do, they open up a worm hole directly into your network through their desktops.

As I mentioned earlier, resisting new kinds of connections to the outside world is futile and can be dangerous to your company. If you try to stop technical advances such as IM and Web conferencing, users will find a way around you, leaving your systems—and your job—less secure. Stay vigilant. Plan ahead. Stay safe.

InstantDoc ID 94763

SharePoint Security Evolution

Follow the maturation of SharePoint 2003 into SharePoint 2007—a new version that will significantly enhance your security infrastructure

by Matt Ranlett and Brendon Schwartz

Microsoft SharePoint Services 2003 has evolved into Microsoft Office SharePoint Server 2007, offering a much fuller, richer security toolset. Whereas SharePoint 2003 relied on logon security backed by Active Directory (AD), portal security, and list-level security, SharePoint 2007 improves previously existing security features while adding auditing features, storage policies, and secure collaboration products such as Excel Services. Let's take a look at how security has evolved in SharePoint, how each version tackles authentication and authorization, and how SharePoint 2007 will benefit your organization.

SharePoint 2003 Authentication

Let's start by taking a closer look at the security features of Microsoft's SharePoint 2003 products and technologies. The foundation of any secure product is the ability to control access to secured materials—which essentially boils down to digital identity and passwords. Because SharePoint 2003 technologies rely on AD to provide user-account validation, the password policies of any SharePoint site are basically the password policies of the underlying AD network. As the *Microsoft SharePoint Products and Technologies Resource Kit* points out, password policies need to take a host of recommendations into account, particularly when you're considering the addition of SharePoint technologies to a network. These recommendations include minimum password length, password complexity, limits on consecutive password attempts, prohibition of sharing passwords, and smart card or biometric device usage.

What exactly does the reliance on AD mean in terms of user authentication (verifying that users are who they claim to be)? SharePoint 2003 offers two modes of operation: *preexisting-account mode* and *account-creation mode*. In the preexisting-account mode (aka *domain mode*), an AD account must exist before a user can access a SharePoint site. In the account-creation mode (selected during SharePoint installation) you can have an AD account automatically created each time you add a new SharePoint user. If you're unsure which mode you're in, you can use the included Stsadm.exe command-line tool to find out.

In either case, the existence of this AD account provides the authentication necessary to access SharePoint. SharePoint validates the existence of the user in AD either through NTLM or Kerberos protocols. To provide authorization, the system compares the authenticated account with a list of access-control information for the SharePoint site itself. These authorization lists are stored in Microsoft SQL Server content databases and are modified from within SharePoint. You can organize these lists or groups at the user level, in site-level groups, or in multisite level groups.

(I've just stated that SharePoint relies on AD to provide account validation, but that's not 100 percent accurate. You can also use local Windows accounts. However, if you don't use AD, you lose the ability to pre-populate the SharePoint profile database. And if any users have personal sites, they won't be registered for cross-farm synchronization in a server farm environment. Because of these severe restrictions, AD environments are highly recommended.)

SharePoint 2003 Authorization

What does the reliance on AD mean in terms of user authorization (validating that users have permissions to access a resource)? SharePoint 2003 authorization is based on groups of rights to

Learning Path

WINDOWS IT PRO RESOURCES:

"Integrate SharePoint into Your Exchange Environment," InstantDoc ID 93701

"Bringing SharePoint to Outlook," InstantDoc ID 93700

"Planning Your SharePoint Portal," InstantDoc ID 93100

"Making Sense of SharePoint Portal Server Architecture," InstantDoc ID 93082

"Types of SharePoint Sites," InstantDoc ID 50624

"SharePoint Tips and Techniques," InstantDoc ID 50540

"7 Things You Need to Know About SharePoint Services," InstantDoc ID 49873

"14 Things You Need to Know About SharePoint Portal Server," http://www.windowsitpro.com/needtoknow

MICROSOFT RESOURCES:

Microsoft SharePoint Products and Technologies Resource Kit
http://www.microsoft.com/technet/windowsserver/sharepoint/V2/reskit/c2461881x.mspx

Microsoft Office SharePoint Server 2007
http://www.microsoft.com/office/preview/servers/sharepointserver/overview.mspx

Microsoft SharePoint Products and Technologies Team Blog
http://blogs.msdn.com/sharepoint

WEB RESOURCES:

SharePoint Blogs
http://www.sharepointblogs.com/

"How can I tell if WSS is in Account Creation Mode?"
http://wss.collutions.com/Lists/FAQ/DispForm.aspx?ID=151

which specified users or groups of users are assigned. You can easily customize security groups, but by default five security groups ship with Windows SharePoint Services:

- Administrator—Wields complete control over the Web site
- Web Designer—Controls the look and feel of the Web site
- Contributor—Can add content to existing Web Parts
- Reader—Has read-only access to content in lists and document libraries
- Guest—Holds the lowest levels of permissions. This group is designed to give read access to sub-portions of a site without giving access to the entire site.

The rights fall into three general categories: *list rights, site rights,* and *personal rights*. The system checks list rights to determine whether a user is able to contribute to a list, edit list items, manage columns in a list, and so on. The system checks site rights whenever a user attempts to create a site, manage a site's users, change the look and feel of a site, and more. The system checks personal rights when a user tries to create or change a personal list view and use private or personal Web Parts. Figure 1 shows the full list of available rights in SharePoint 2003.

After you grasp how your SharePoint system organizes its rights into groups, you'll understand how to organize your users. It's possible to individually manage each user's permissions, but creating groups to hold your users is the recommended best practice. You have two options for grouping your users: *site groups* and *cross-site groups*. A site group is a group of users available for assignment on that particular SharePoint site. If your users are grouped in a cross-site group, the system actually creates that group at the top level for the site collection, and it's available to any site in that site collection.

Suppose your organization, Contoso, has several departments, such as Marketing, Executive, Finance, and IT. If each of these departments has its own site under the top-level Contoso site, a user in the Executive department might not have access to documents stored by the Finance department unless he or she is explicitly granted those rights. However, if the users for each department reside in cross-site groups, the manager of the Finance department has to grant only the Executive cross-site group read access to its portal, and all members of the team can be admitted at once.

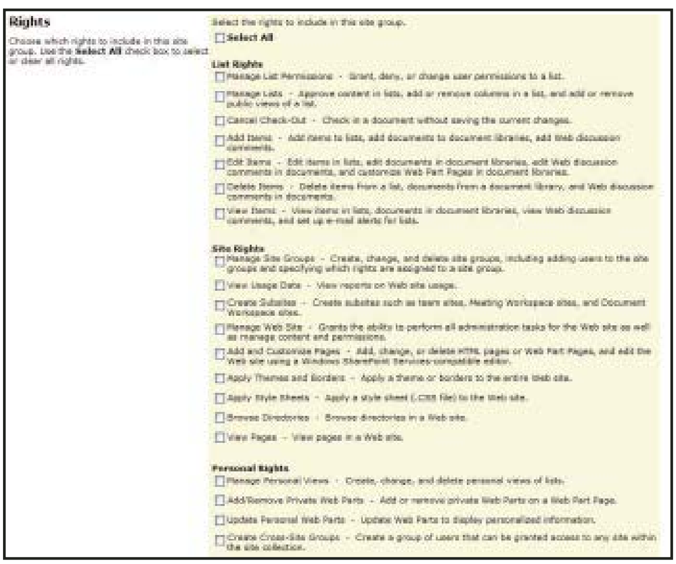


Figure 1:
Available rights in SharePoint 2003

Site-Level Security

Now, you have groups of users and groups of rights. What can you do with these groups to secure the SharePoint portal? SharePoint 2003 offers two levels of security: *site level* and *list level*.

When you create a SharePoint site, you—as the creator or owner—have a choice about how to handle security. The options are to inherit the permissions of the parent site or to use unique permissions. If you decide to inherit the parent's permissions, the security options flow down to the new portal site and everyone who has any level of access in the parent site has the same level of access in the new site. If you select unique permissions, you are initially the only user given any access to the new portal site. After the site's creation, you can add new users or groups of users to the site and can grant specific permissions.

Suppose your Contoso organization has an IT department. The IT department wants to grant employees the ability to track trouble tickets through their SharePoint issue-tracking list. To that end, the IT department has created an IT portal site off the main Contoso site. In this fictional organization, every member of the domain has at least read access at the main company site. When you created the IT portal site, you did so with inherited permissions; any domain user has the ability to connect to the IT portal site and see the data on the home page, including the issue-tracking list on the IT portal site's home page. Now, the IT department needs to have a location at which it can save IT-specific information, such as server passwords. The IT department doesn't want users to see that this documentation exists, so it has

Figure 2:
Granular rights in SharePoint 2003

created a new portal site with unique permissions. This PrivateIT portal site might have only members of the IT department as users. When non-IT users attempt to access the PrivateIT portal site, they'll see an error message stating that they don't have permission to access that resource. Optionally, you can have the system prompt them with a message stating that they can ask the administrator to grant them access to the restricted portal.

List-Level Security

List-level security works similarly, but at the individual list level as opposed to the site level. Consider again the example of the public IT portal site with its issue-tracking list. Suppose the IT department wants to give any user the ability to read items in the list, but the department wants to give members of the Managers cross-site group the ability to add new issues and edit existing issues. In the list's permissions options, you can add users or groups and assign them various permissions. You simply enter the list, click *Modify Settings and Columns*, and click the *Change permissions for this list* link. Figure 2 shows the most granular list of rights available for assignment. You might notice the tantalizing *Modify item-level security* link in the left pane. This link offers you only the ability to toggle users' views from seeing and editing all entries in the list to seeing only their own entries in the list.

This item-level permission is a hint of what is to come in SharePoint 2007, which represents a major evolution in terms of authentication and authorization over that which SharePoint 2003 offers. Choices are more diverse, more granular, and more intuitive.

SharePoint 2007 Authentication

In SharePoint 2007, you not only have the same Windows-integrated options as before—you also have the ASP.NET provider model. Use of the ASP.NET provider model removes the need for AD or Windows accounts and gives you new options, such as forms authentication against any store of user data (e.g., a SQL Server database). You also have the option to use Web-based single sign-on (SSO) options in which the user is logged on via a non-SharePoint logon form. A familiar example of a Web-based SSO option is Windows Live ID (formerly known as .NET Passport). This authentication evolution gives developers and administrators much greater flexibility while installing and configuring SharePoint 2007.

SharePoint 2007 Authorization

The SharePoint authentication changes are important, but they're not nearly as big as the forthcoming authorization improvements. In SharePoint 2003, users and administrators are concerned with *rights*, but in SharePoint 2007, the term is *permissions*, and the division between groups of users and groups of permissions is much more clearly defined. People are assigned to logical groups, such as IT managers, junior finance employees, and executive team members. Permissions are assigned to logical groups, such as designers and readers, and the permissions associated with those groups are clearly defined. In SharePoint 2003, distinction is blurred. At the site level, you might assign a person to the Readers role, but at the list level, the Readers group acts more like a rights specification. In SharePoint 2003, this dynamic leads to confusion among administrators: Which group of users is allowed to do what in each site and in each list?

Another major security improvement in SharePoint 2007 is the addition of

Figure 3:
The Quick Nav bar

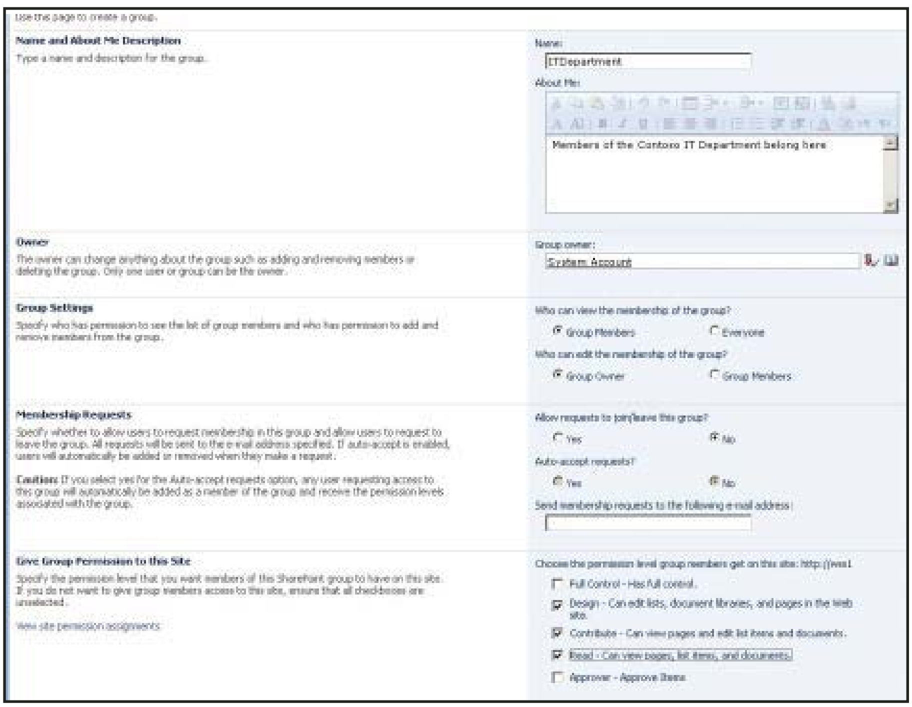


Figure 4:
Adding a new group

Figure 5:
Adding a new permission level

finer-grained permissions. Now, not only can you secure a site or list, you can also secure a folder and an item in that list. Therefore, you can use the same library to store sensitive documents and publicly available documents. To prevent unauthorized access attempts, SharePoint 2007 offers a security-trimmed interface. If a user doesn't have permission to view a document or menu item, that document or menu selection doesn't even appear to that user. The entire Site Actions menu won't appear if the user doesn't have the required permissions to use any of the menu's elements.

SharePoint Groups are logical groupings or collections of people. Out of the box, the software offers three groups: Owners, Members, and Visitors. These groups function like SharePoint 2003's cross-site groups in that you can assign them anywhere in a site collection and they will be henceforth available for use anywhere in that site collection. These groups let you scale permission assignments across large numbers of people.

The original concept of SharePoint site groups is extremely flexible, making it difficult to effectively organize users and roles. You can assign users to a site group, and you can assign rights to the site group. Then, by assigning the site groups of users to those groups that contain rights, you effectively create a role by defining which users can do specific actions. The new version addresses this ambiguity in the definition and purpose of groups. In SharePoint 2007, the role-based concept of collections of permissions is now clearly defined as a permission level, which functions as a role. You assign permissions to these permission levels, and you assign these permission levels to SharePoint groups.

Groups are also now always defined at the site-collection level, enforcing a consistent naming convention within all the sites of a site collecction. All of this reduces the potential for confusion.

Consider a hands-on example. In a SharePoint portal, click the *People and Groups* link in the Quick Nav bar, which Figure 3, page 59, shows. Click More to view all your groups. By doing so, you see that your site has only the default groups available. You want to add two new groups to represent your Contoso IT department users and your Finance department users. Click New, and select New Group from the drop-down list. For the IT department, fill out the form that you see in Figure 4, page 59. Notice the permission levels at the bottom of the form. Before you go on to add a group for the Finance department, create a new security permissions level for the Finance users. Back in the list of groups, click Site Permissions to access the screen that Figure 5 shows. On this screen, you can see the permission levels and groups to which the Finance users are assigned, and you can manage the many-to-many relationship between groups and permission levels. You can see that the roles of Read, Contribute, and Full Control (i.e., administration) exist, along with the new SharePoint 2007 levels of Limited Access (equivalent to SharePoint 2003's Guest level) and Approver. To add a new permission level for your Finance team members, click Settings, Permission Levels. A list of available permissions will appear. Click *Add a Permission Level* to create a new Finance user role. On the screen that Figure 6 shows, you can see how many more permission options are available in SharePoint 2007 than in SharePoint 2003. Select the permissions you want (grant lots of list rights) and click Create. Now, you have a new permission level for Finance department employees. Go back to your Permissions home page and add a new group to contain your actual Finance employees. When you do so, the added Finance user permission group will appear at the bottom of the New Group screen. Now, you can add users to the Finance group, and any user of the Finance group will have the same permissions in any site in the SharePoint site collection.

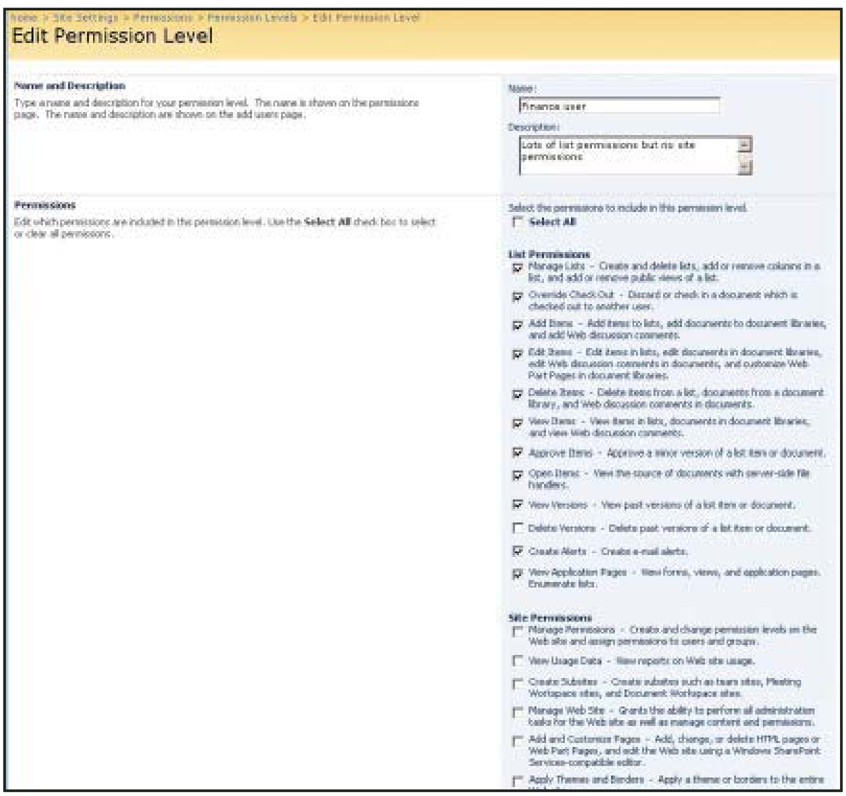


Figure 6:
Permission options available in SharePoint 2007

Now that you understand how to collect users into groups and how to assign the groups various permissions, you can see how you'll use these groups to secure SharePoint 2007. Just as in SharePoint 2003, you can explicitly grant or deny access to a site or a list, but you now have the additional ability to secure individual list items and document library folders. So, a user might have access to a site and a document library, but you can have individual documents or folders to which the user has no access.

Administrative Security

This has been a discussion of user-level and site-level security in SharePoint 2003 and SharePoint 2007. There are additional levels of security available to SharePoint administrators, who can also apply security at the Shared Services level and at the Central Administration level in SharePoint 2007.

Shared Services isn't a new concept, but it's now much more apparent. Essentially, Shared Services administration means that the server-farm administrator can delegate authorization for certain tasks to other users. This capability is handy when users make unwanted changes, such as item deletions (and subsequent Recycle Bin clearing). Now, with delegated user authorization, the user doesn't have to go to the farm administrator for help.

The final possible level of security configuration in a SharePoint 2007 installation is at the Central Administration level. There are a lot of new administration features at this level, including security policies—a set of permissions that apply everywhere across the farm. These Grant and Deny policies override all other permissions, and you can configure them per Web application and per Web zone. Common examples of security policy use include granting full read access to auditors and denying all write access to anyone in the Internet zone (i.e., Extranet). You can also set up the AD service accounts at this level to prevent unauthorized application behavior on the network. You configure the application pool accounts, the SharePoint service (SPTimer and Admin Service) accounts, and access to SQL Server at this level.

A Powerful Force

SharePoint 2007 is poised to greatly improve the SharePoint end-user experience. Thanks to a slicker interface and features such as security trimming, the user will see only the sites, lists, and documents that they have permission to see. More important, SharePoint 2007 will simplify the life of the administrator, thanks to cleanly organized users and roles defined at one level, the ability to delegate activities to others via Shared Services, and the introduction of system-wide security policies.

InstantDoc ID 94335

Matt Ranlett
(mranlett@devcow.com) is a consultant with Intellinet in Atlanta. Matt is a Microsoft MVP, co–vice president of Technology for INETA, and cofounder of the Atlanta .NET Regular Guys.

Brendon Schwartz
(bschwartz@devcow.com) is a senior consultant in Atlanta. Brendon is a Microsoft MVP, co–vice president of Technology for INETA, and cofounder of the Atlanta .NET Regular Guys hosted at DevCow (http://www.devcow.com).

SharePoint Server 2007 Unleashed

Experience firsthand the power of SharePoint

by Dan Holme

Microsoft Office SharePoint Server 2007. What a mouthful. And what a handful. First, let's take care of the mouthful—the product is often referred to as SharePoint Server, just SharePoint, or MOSS. I'll refer to it as SharePoint Server or SharePoint Server 2007. As for the handful, SharePoint Server addresses an exceptionally broad range of business scenarios by delivering capabilities in six categories: Portal, Enterprise Search, Collaboration, Business Intelligence, Business Process, and Content Management.

Whether you're new to SharePoint Server and want to learn what business value it offers your organization, or you've experienced earlier versions of SharePoint Server and want to see what 2007 brings, I'd like to guide you on a journey into SharePoint Server 2007 through seven "experiences":

1. Obtain and install SharePoint Server 2007.
2. Configure the top-level site.
3. Create a departmental site.
4. Create a document library.
5. Subscribe to changes in the library by using RSS.
6. Take the library offline through Microsoft Office Outlook 2007 integration.
7. Generate a repository for standard Microsoft Office PowerPoint 2007 slides.

However, before we dive in, let's get a quick overview of SharePoint technology.

What Is SharePoint Server 2007?

SharePoint Server 2007 is a server product that's part of Microsoft Office System 2007. It sits on top of Windows SharePoint Services 3.0, which I examined last month in "Windows SharePoint Services 3.0 Out of the Box," InstantDoc ID 94240. SharePoint Server leverages Windows SharePoint Services 3.0's plumbing and adds its own significant functionality. Figure 1 shows some of SharePoint Server's Web application features. Some of these features—such as forms services, Excel Services, and the Business Data Catalog—are exclusive to the Enterprise version. The rest are included in the Standard version.

As you approach SharePoint Server, you might find, as I did, that its full capabilities are somewhat mind-blowing. I had to work with SharePoint Server piece by piece, getting acquainted with its features gradually. That's why I've created these "experiences"—to help you learn as we create our SharePoint Server sandbox for a fictional organization, WINDOMAIN.com.

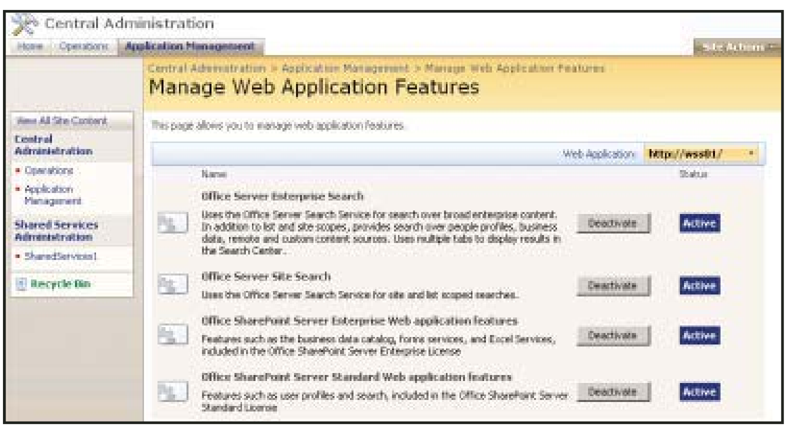


Figure 1:
SharePoint Web application features

Experience 1: Obtaining and Installing SharePoint Server 2007

1

The most important SharePoint Server–related URL for you to know is http://office.microsoft.com/sharepointserver. This URL will get you to the SharePoint Server Web page, from which you can locate documentation, support, and (as of this writing), a downloadable trial of both the Standard and Enterprise editions of SharePoint Server 2007.

Download the trial version of SharePoint Server, as well as Microsoft .NET Framework 3.0, which you can access from the .NET Framework page at http://msdn2.microsoft.com/netframework. I recommend using a "clean" server for your sandbox, to eliminate any idiosyncrasies that might otherwise cause problems. Log on to your soon-to-be SharePoint Server system with a user account that's not the Administrator account but that is a member of the Administrators group. The account you use to install SharePoint Server becomes the default "owner" of the site collection and its sites.

Install .NET Framework 3.0, then install SharePoint Server. There's no rocket science to either of the installations. The only choice you need to make is the type of SharePoint Server installation. For our purposes, choose Basic installation. This installation takes care of the configuration of the server farm, the server, the applica-

tions, and the shared services. However, for a production installation, you'll more likely choose the Advanced installation so that you can manually configure the components and set up your single server in anticipation of eventually increasing to a farm of multiple servers. With the Basic installation, the standalone server can't later become part of a multiserver farm.

When installation has completed, you'll be prompted to run the SharePoint Products and Technologies Configuration Wizard. If you don't run it now, you can launch the wizard from the Administrative Tools folder on the SharePoint server. The wizard performs a series of tasks depending on the type of installation you've performed. When the wizard finishes, it informs you of your next step.

In the Administrative Tools folder of your SharePoint Server system, open the SharePoint Central Administration application. The SharePoint Central Administration Web page will appear. This is where you'll perform most of the administration of SharePoint Server. Make a note of the URL for the site—it will be your server name with a randomly assigned port number, such as http://wss01.windomain.com:22222. Now you can open the same site from any machine on the network by using the full URL that includes the port. If you're prompted to authenticate, use the account you used when installing SharePoint Server, in the form DOMAIN\username. You'll need to add the Central Administration Web site to your Trusted Sites zone to ensure proper functionality. Feel free to poke around and see what has been configured, but don't change anything just yet—the Basic installation already configured what was needed at this point.

Experience 2: Configuring the Top-Level Site

Open the SharePoint Server site by using the URL http://*servername* (e.g., http://wss01). The default home page appears, which you can see in Figure 2.

The Basic installation you performed created a site collection. A site collection contains one or more sites, each of which can inherit security policies, settings, templates, and user and group definitions. In many production implementations of SharePoint Server, one site collection will suffice. You'll typically have a top-level intranet portal with-

Figure 2:
Default Home page, People And Groups menu

in which you'll create sites for departments, functions, teams, or projects.

SharePoint Server 2007 doesn't use the *areas* concept that Microsoft SharePoint Portal Server 2003 uses. SharePoint Server 2007 uses *sites*, a term that's more intuitive and effective. By default, sites are represented as tabs in the global navigation panel at the top of each page. Figure 2 shows tabs for several sites created by default when you install SharePoint Server 2007: Document Center, News, Reports, Search, and Sites. Also, you'll see at the left on every page a site navigation panel that contains the Quick Launch bar and/or a tree view, based on the site's settings. This is a welcome change from previous versions, in which the Quick Launch appeared only on the default page.

For guidance about how you can customize and brand SharePoint Server, check out "Windows SharePoint Services 3.0 Out of the Box." For this article, I focus on functionality. Because SharePoint Server is all about collaboration and access to information, you need to open the site to your users. Click the Site Actions button in the upper-right corner of the page, and choose Site Settings, People And Groups (as Figure 2 shows).

On the People And Groups page, select Home Members in the left panel, then click New, and choose Add Users. Here is where you specify the members of this site by associating permissions with members and other default groups. You can experiment with locking down your top site later, after you've studied the planning and deployment guides, but I suggest you add your users to the Members group for now so that their My Site configuration, which I plan to describe in a future article, is easier to do.

On the *Add Users: Home* page, select *Add all authenticated users.* This configures the group to include all authenticated users—that is, all of your domain's users. For our fictitious organization, WINDOMAIN.com, the users include Colleen Outyall, director of communications; Penny Xavier, budget manager; and yours truly, Dan Holme.

Experience 3: Creating a Departmental Site

As I mentioned above, the default installation creates several functional subsites, including Document Center, News, Reports, Search, and Sites. I want to create a site for the communications department. Colleen's team wants to collaborate but also needs a way to distribute company brochures to the sales and marketing teams. I start by returning to the Home page and, from the Site Actions menu, choosing Create Site. The New SharePoint Site page (in Figure 3, page 64) appears. This is where you configure the title, URL, template, and permissions for the new site.

Enter "Communications" as the title and "communications" as the URL. Select the Team Site template (the default). Under User Permissions, select *Use unique permissions.*

Using unique permissions is important: you might want some users to contribute to a departmental site but not to the corporate or parent portal, and vice versa. With SharePoint Server 2007's security model, each new site inherits the parent

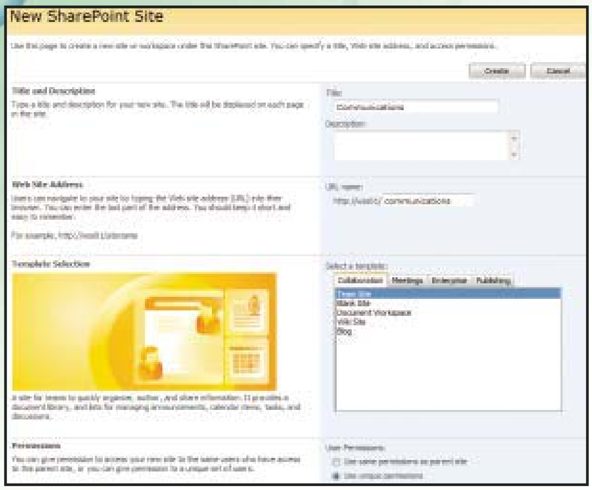


Figure 3:
The New SharePoint Site page

can "break" that inheritance while creating a site, as we're doing now, or you can reconfigure permissions later for an existing site by using the permissions section of Site Settings. One nice feature of the SharePoint Server security model is that group definitions belong to the site collection, so if one group requires certain permissions across several sites, you need define the group only once, then give it appropriate permissions in each site.

When you specify *Use unique permissions* during site creation, you're sent to the *Set Up Groups for this Site* page, which Figure 4 shows. You can define Visitors, Members, and Owners by using either a group previously defined in the site collection or by creating a new group and specifying the members. The members can be users or groups, and the SharePoint Server "picker" makes it easy to search your domain for those accounts. It's worth noting that SharePoint Server doesn't have to use Active Directory (AD) and the local SAM database as its source of user and group accounts: It can use any .NET Membership Provider, including ASP.NET 2.0's SqlMembershipProvider. A discussion of such "forms-based" or custom membership providers is beyond the scope of this article, but you should still know about them because at some point, you'll probably need to open part of your SharePoint Server infrastructure to partners, customers, or others without domain accounts.

Experience 4: Creating a Document Library

Now that you've created the Communications site, let's create a document library for the corporate brochures. On the Communications home page, select Site Actions, Create. Click Document Library, and give the library a name: I chose "Marketing Communications." On the *New document library* page, you can also turn on versioning, which preserves the history of changes made to a document so that you can open previous versions. For corporate marketing communications documents, it makes sense to preserve previous versions, so turn on versioning.

Experience 5: RSS

SharePoint Server lists and libraries are wired for RSS, thanks to Windows SharePoint Services. In the Marketing Communications library, which Figure 5 shows, click the Actions button and choose View RSS Feed. Use your preferred RSS reader to subscribe to the feed. I used the built-in RSS capability of Microsoft Internet Explorer (IE) 7.0.

Return to the Marketing Communications library and upload a document. Then check the RSS feed. You should see your document in the RSS feed within minutes.

Experience 6: Outlook Integration—SharePoint's Answer to Public Folders

When you add Office applications to the SharePoint mix, you get even more functionality. Office 2003 applications do a good job of integrating with SharePoint Server, but Office 2007 applications integrate even better. As you walk through a demonstration of Outlook 2007 integration with SharePoint Server, you're bound to elicit "oohs," "ahhs," and "wows" from your team and management. You'll also get a glimpse into how Microsoft is moving toward replacing public folders with SharePoint.

In the Marketing Communications library, click Actions and choose *Connect to Outlook*. The document library will appear in your Outlook folder hierarchy and will be synchronized based on your Send/Receive settings. Figure 6 shows the uploaded brochure within Outlook—Outlook made it available offline automatically.

Experience 7: Slide Libraries

Give this experience a try if you have access to PowerPoint 2007. From the Communications home page, select Site Actions, Create. This time, choose Slide Library and give the library a name. I chose "WINDOMAIN.com slides," but it would be wiser to keep names restricted to alphanumeric characters and spaces because SharePoint Server deletes periods.

In PowerPoint, create a presentation with several slides and save it. Then, in the slide library, click Upload and choose Publish Slides (you can also publish from the Office menu in PowerPoint). You'll be asked which presentation to publish, and you'll be given the chance to select specific slides. When you're done, refresh the slide

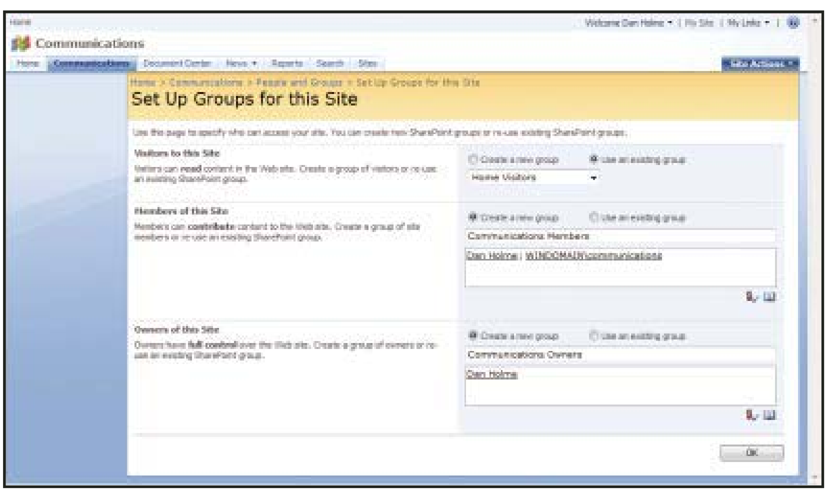


Figure 4:
Set Up Groups for this Site page

IMMERSIVE EDUCATION FROM MICROSOFT AND THE WORLD'S TECHNOLOGY EXPERTS

- Choose from over 150 in-depth, no-hype sessions delivered by Microsoft and industry experts.
- Dive into Microsoft Exchange Server 2007's new security, administration, and unified messaging features, and how you can integrate it with your existing network resources.
- Get the insiders scoop during dynamic keynotes and general sessions on Windows Vista, Exchange Server 2007, Microsoft Office 2007 and Microsoft SharePoint 2007 technologies.
- Attend the hands-on Exchange troubleshooting and Windows scripting labs.
- Get answers to your challenges and questions in our Meet the Experts lounge!
- If you're planning any sort of migration, learn the tips and tricks based on real-world experience before you start.
- Explore the partner exposition, pick up great giveaways, and enter the Harley-Davidson motorcycle contest.
- Gain insights from other participants who represent experienced IT professionals from other companies.
- Unwind and network with your peers at a world-class Orlando resort.

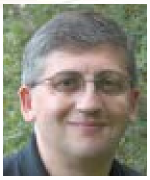
TABLE OF CONTENTS

SCHEDULE AT A GLANCE

SUNDAY, APRIL 1, 2007	
7:00 am - 6:00 pm	Conference Registration
9:00 am - 4:00 pm	Pre-conference Workshops
6:30 pm - 8:30 pm	Opening Keynote
8:30 pm - 10:00 pm	Expo Hall Opens
MONDAY, APRIL 2, 2007	
7:00 am - 6:00 pm	Conference Registration
7:00 am - 8:00 am	Continental Breakfast
8:00 am - 9:00 am	Keynote
9:30 am - 10:30 am	Conference Sessions
10:45 am - 11:45 am	Conference Sessions
11:45 am - 1:30 pm	Lunch
1:30 pm - 2:30 pm	Conference Sessions
2:45 pm - 3:45 pm	Conference Sessions
4:15 pm - 5:15 pm	Conference Sessions
TUESDAY, APRIL 3, 2007	
7:00 am - 6:00 pm	Conference Registration
7:00 am - 8:00 am	Continental Breakfast
8:00 am - 9:15 am	Conference Sessions
10:00 am - 11:15 am	Conference Sessions
11:30 am - 12:45 pm	Conference Sessions
12:45 pm - 2:15 pm	Lunch
2:15 pm - 3:30 pm	Conference Sessions
4:15 pm - 5:30 pm	Conference Sessions
WEDNESDAY, APRIL 4, 2007	
7:00 am - 8:00 am	Continental Breakfast
8:00 am - 9:15 am	Conference Sessions
9:30 am - 10:45 am	Conference Sessions
11:30 am - 12:30 pm	Conference Sessions
12:30 pm - 2:15 pm	Lunch
2:15 pm - 3:15 pm	Conference Sessions
3:15 pm - 3:45 pm	Ice Cream Break
3:45 pm - 4:30 pm	Closing Session
THURSDAY, APRIL 5, 2007	
9:00 am - 4:00 pm	Post-conference Workshops

SEE WEB SITE FOR THE LATEST SCHEDULE UPDATES.
www.WinConnections.com

EXCHANGE 2007: GETTING TO KNOW YOU



TONY REDMOND HP

Exchange 2007 represents the third generation of Exchange server. The migration from the first generation (5.5) to second (2000) posed some problems because of the requirement to deploy the Active Directory and a new architecture for Exchange. The same may be about to happen as we move to Exchange 2007 because the same type of architectural change exists alongside the need to deploy a brand new Windows 64-bit platform. This session covers the essential points that you need to know about Exchange 2007 to help you prepare to deploy the new version, including the many holes that an unwary administrator can fall into.

Tony Redmond is the Vice President and Chief Technology Officer for HP Services. He is responsible for the technology strategy and leadership of HP Services, including the development of the HP Services technology community, including overseeing the implementation of the Technical Career Path (TCP), Professions, and advancing a knowledge culture within HP Services. He is responsible for driving a common R&D and technology leadership across the HP Services business units. Tony is the Security Lead for HP and manages the HP Security Office, which is responsible for setting the strategy and direction for HP's security initiative and coordinating activities across all business units.

ATTACKER TRENDS AND TECHNIQUES: AN UPDATE

STEVE RILEY MICROSOFT

The bad guys just keep getting better! They're constantly changing their tactics and inventing new techniques to cause you harm, damage your data, and make your resources unavailable. Why do they do this? What motivates someone to—let's call it what it is—commit computer-related crimes? How have they changed and improved? What kinds of attacks are popular now and why are they so effective? What might we expect to see in the future? Steve Riley will help you understand the latest in attacker trends and techniques so that you can plan appropriately and implement effective processes and technologies to mitigate their threats.

Steve Riley's career at Microsoft began in 1998 in the telecommunications practice of Microsoft Consulting Services where he worked with several ISPs and ASPs to design highly-available network architectures, develop hosting platforms for various custom and off-the-shelf applications, and deploy complex multi-site VPNs. His specialization in security led him next to the security consulting practice, where he worked with many customers to conduct security assessments and risk analysis, deploy technologies for attack prevention and intrusion detection, and assist with occasional incident response efforts. Steve is now a product manager in Microsoft's Security Business Unit. He is a frequent and popular speaker at conferences worldwide, often appearing in Asia one week and Europe the next; Steve's speaking engagements have included multiple Microsoft TechEds and other conferences, plus SANS, RSA, Black Hat, Windows IT Pro roadshows, and InfoSec US. When not evangelizing the benefits of Microsoft security technology, Steve spends time with customers to better understand the security pain they face and show how some of that pain can be eliminated. Steve's technical specialties include network and host security, communication protocols, network design, and information security policies and process.

LIVING THE LONGHORN LIFE: WHAT'S UP WITH SERVER 2007 (OR MAYBE, 2008)

MARK MIINASI MR&D

Microsoft released the new desktop, Windows Vista, in November 2006… but that's just the start. A new version of Server's right on its heels—formerly code-named "Longhorn Server," it'll either be named Windows Server 2007 or 2008, depending on when it ships. But no matter what its name, Server 2007/8 will pack a ton of new stuff, from some really good news in Active Directory to some nifty new deployment tools, a quarantine system that'll help you keep the worm-ridden systems off of your network, a revamped Web server, and a few truly long-awaited changes in group policy. How can you find out about all of this? Well, you could download a few terabytes worth of white papers and start sifting through them to separate the wheat from the chaff, or you could attend this short session by Mark Minasi, the guy who's been explaining new operating systems since Windows 1.0. Come to this session and find out why Server Core may be your favorite new piece of software!

Mark Minasi is an author, a technology columnist, a commentator, a keynote speaker, and an all-around alpha geek. What separates him from many of the other alpha geeks is that he knows how to explain things to normal humans and often make them laugh while doing it. He's probably best known for his books, ***Mastering Windows NT Server*** (Sybex), ***Mastering Windows 2000 Server***, and ***The Complete PC Upgrade and Maintenance Guide*** and his columns in ***Windows IT Pro***. Mark has also authored 17 other technology books, spoken on technical topics in 20 countries, and written and appeared in a dozen technical education videos. His most recent works are ***Mastering Windows 2000 Server***, Third Edition and ***Mastering Windows XP Professional***. He has also written ***Linux for NT/2000 Administrators*** and a seventh edition of ***Mastering Windows NT Server 4.0***.

SESSIONS AND SPEAKERS ARE SUBJECT TO CHANGE. SEE WEB SITE FOR UPDATES AND ADDITIONAL SESSIONS.

MICROSOFT EXCHANGE

SESSIONS PRESENTED BY MICROSOFT

It's the all-new, rearchitected, more powerful messaging and groupware platform from Microsoft: **Exchange Server 2007!** Packed with new features, new architectural options, and new capabilities, Exchange Server 2007 is also the first fully automatable and command-line-managed server product from Microsoft, leveraging the Windows PowerShell shell and scripting environment. Rely on Exchange Connections to connect you with the most respected and relied-upon subject-matter experts in the world for Exchange Server 2007. **Come to Exchange Connections to:**

- Learn about new architecture options in Exchange Server 2007, including ways of scaling out your Exchange Server environment bigger and better than ever before.
- Discover how Exchange Server 2007 works under-the-hood, including data management, engine details, troubleshooting and disaster recovery, and much more.
- Provide your users with anywhere e-mail access through an all-new Outlook Web Access, mobile e-mail access, and much more.
- Keep your Exchange Server 2007 environment secure with information on internal security, antivirus, anti-spam, and other measures that keep your environment and your users safer.
- Learn about deployment and migration techniques and issues, making your Exchange Server 2007 migration and deployment easier, safer, and faster.

EXCHANGE CONNECTIONS COVERS THE TECHNOLOGIES YOU NEED:

DISASTER RECOVERY
- Continuous Backup
- Standby Cluster Recovery
- Online Backup Recovery

SECURITY
- Sender ID
- Creating and Testing Mail Hygiene

TROUBLESHOOTING
- Troubleshooting Message Flow
- Troubleshooting DNS
- Advanced SMTP Troubleshooting

MIGRATION AND DEPLOYMENT
- Migration Issues
- Deployment Techniques
- Performance Optimization

END-USER FEATURES
- Client Access Server
- Small Business Mobility
- Getting Rid of PSTs

MICROSOFT EXCHANGE SERVER 2007: THE NEXT GENERATION OF EXCHANGE

Exchange Server 2007, the next major version of Exchange, will be a leap forward in enhancing the information worker's access to larger mailboxes while giving the e-mail administrator a more manageable and secure e-mail infrastructure. In this session, we provide an overview of the product direction and provide a sneak peak at some of the new features that will be included in the product.

MAIL THAT SPEAKS TO YOU: UNIFIED MESSAGING IN MICROSOFT EXCHANGE SERVER 2007

Microsoft is integrating Unified Messaging natively into Exchange Server 2007. In this session you will learn the features, benefits, and architecture of Exchange Unified Messaging. See how Exchange can take voice mail and fax messages, how you can call in over any phone to access your voice mail, e-mail, calendar or contacts, how you can build automated attendants, and how speech access is integrated into the product. Learn how easy it is to configure and deploy Exchange Unified Messaging for your organization.

GETTING STARTED WITH MICROSOFT EXCHANGE SERVER 2007: SIMPLE INSTALLATION, SETUP AND ADMINISTRATION SCENARIOS

Exchange Server 2007 is now built on standard Microsoft installer so that you can take advantage of patching services such as the Software Update Service (SUS). Exchange Server 2007 supports new server roles for flexible deployment of the topologies you require and the power to automate installation. These are just some of the new advancements in the Exchange Server 2007 set-up experience. This is a must-see session for a high-level overview and walkthrough of how you will be deploying Exchange 2007.

EXCHANGE 2007 ARCHITECTURE AND DESIGN

Ever wondered how a large enterprise plans and implements design and architecture of its next generation of messaging system? Join us in this session where engineers from the Microsoft IT messaging team will uncover the details on how Exchange 2007 infrastructure was introduced and fully deployed in a 120,000+ mailbox production environment. Topics will include: messaging topology design, hardware planning for various Exchange server roles, client access server and mobility scenarios, transport architecture, mailbox server and storage designs, backup, restore and high availability strategies.

MANAGING EXCHANGE SERVER 2007: THE NEW EXCHANGE MANAGEMENT CONSOLE AND SHELL

Imagine having a toolset that is flexible enough to easily deploy and administer a single Exchange server and yet powerful enough to completely automate those same actions for hundreds of servers. Yes, you heard right, Exchange Server 2007 will deliver a new intuitive GUI experience allowing you to quickly provision Exchange functionality while the new command-line experience will allow you to automate your world. This session is loaded with demonstrations showing off the new Exchange 2007 toolset and also highlights the underpinnings of this new revolutionary architecture which is built on the groundbreaking Windows PowerShell technology.

MOBILE ACCESS TO EXCHANGE 2007 AND LIVE COMMUNICATIONS SERVER ANYTIME, ANYWHERE, AND ON ANY DEVICE!

Do you need to provide anytime, anywhere access to Exchange 2007 and Live Communication Server in your organization? This session will cover the enhancements in Exchange 2007 for Windows Mobile devices as well as the improvements in Outlook Web Access as well as the future mobile messaging capabilities of Exchange 2007. We will also investigate how to deliver Live Communication Server's capabilities to mobile users.

MESSAGE SECURITY AND HYGIENE IN EXCHANGE SERVER 2007

Out of the box, Exchange Server 2007 customers will find a solution that helps protect their messages and messaging infrastructure from unwanted spam, viruses, and hackers. You'll learn how Exchange Server 2007 uses Kerberos and Transport Layer Security (TLS) to authenticate and encrypt mail within your network, and how message hygiene—including anti-spam and antivirus have been implemented in Exchange Server 2007. You'll also see how Administrators can maintain their network by adjusting spam and virus settings and implementing the appropriate security policies, as well as how end users can use simple and familiar interfaces to recover junk e-mail and apply message classifications.

EXCHANGE HOSTED SERVICES

E-mail is the lifeblood of business, and enterprises rely on IT to keep their communication arteries secure, protected, and compliant. Spammers, hackers, virus-writers, regulators, and spies are making the IT challenge increasingly difficult, further taxing the limits of already resource-strained staff. Attend this session to learn how Microsoft Exchange Hosted Services provides customers with a compelling solution against these types of attacks. We'll review the business drivers impacting you and how you can deploy and administer this managed solution.

EXCHANGE 2003 BEST PRACTICES FROM MICROSOFT IT

Drawing on its tremendous experience with Exchange 2003 architecture, design, and operations, Microsoft IT has developed comprehensive and highly effective best practices to design, run, and maintain its Exchange environment. These best practices are the foundation of the Exchange Center of Excellence, an initiative to reduce customer issues and mis-configurations. This session summarizes how Microsoft IT designed its Exchange 2003 infrastructure and successfully ran it for several years before moving to Exchange 2007. Topics include the Microsoft IT Exchange site consolidation story, cluster design, backup/restore methodology, mobile messaging infrastructure design practices, Internet gateway, and e-mail hygiene solutions.

CO-EXISTENCE AND MIGRATION OF LOTUS NOTES/DOMINO MESSAGING TO THE MICROSOFT PLATFORM

This session provides you with up-to-date information on the tools and guidance you need to move from Lotus Notes/Domino to the Microsoft Collaboration Platform. This session covers co-existence and migration of the Domino directory, messaging, and applications.

THE UNIFIED COMMUNICATIONS TECHNICAL VISION AND STRATEGY

This session will outline Microsoft's vision and technology strategy for Unified Communications. Come and hear directly from Microsoft's Unified Communications leadership about our roadmap and priorities for bringing together business communications infrastructure and user experience. If your organization is considering its strategy for e-mail, voice mail, instant messaging, telephone/VoIP, and conferencing, this session will provide you with Microsoft's approach to addressing these critical organizational needs and improve the modern organization's ability to communicate and collaborate.

INTEGRATING YOUR LEGACY PBX AND NEXT GENERATION VOICE INFRASTRUCTURES WITH MICROSOFT OFFICE LIVE COMMUNICATIONS SERVER 2005, OFFICE COMMUNICATIONS SERVER 2007, AND EXCHANGE SERVER 2007 UNIFIED MESSAGING

If you want to learn about how to integrate your existing voice infrastructures with Exchange Server 2007 and Office Communications Server 2007 (or Live Communications Server 2005), then come to this highly interactive session where you can get your tough questions answered by Microsoft experts.

SESSIONS AND SPEAKERS ARE SUBJECT TO CHANGE.
SEE WEB SITE FOR UPDATES AND ADDITIONAL SESSIONS.

DIVE INTO THE NEW RELEASES WITH MICROSOFT ARCHITECTS AND INDUSTRY EXPERTS!

MICROSOFT EXCHANGE
CONFERENCE SESSIONS

HOW DO YOU MIGRATE FROM A 250,000 MAILBOX EXCHANGE 2003 ENVIRONMENT TO EXCHANGE 2007?
STAN FOSTER

HP's e-mail environment is well distributed and supports over 250,000 mailboxes. HP has always worked closely with Microsoft on Exchange beta programs and was deploying Exchange 2007 internally long before the product hit the streets. But deploying Exchange 2007 to such a large organization as HP's is not as easy as simply slotting the DVD into the drive and running Setup. In this session, we'll describe the mechanisms and processes involved in such a large-scale migration.

REAL-LIFE DEPLOYMENT OF EXCHANGE 2007 UM. LEARN WHAT IT TAKES TO GET THERE
LARRY RIBA/STAN FOSTER

Deploying the Unified Messaging functionality of Exchange 2007 into a real-world environment is a lot different than simply installing the UM role on a standalone server. In this session, the speakers will describe their experiences of deploying UM in a large-scale Exchange environment to support a evaluation of UM for selected users.

WINDOWS SERVER CLUSTERS FOR EXCHANGE ADMINISTRATORS
JUERGEN HASSLAUER

This session provides an overview of clustering services within the Windows operating system. With Exchange Server 2007 you have to set up a Majority Node Set (MNS) cluster if you want to use Cluster Continuous Replication (CCR). You also have to understand the file share witness feature if you want to deploy CCR. Another option with Exchange Server 2007 is deploying a Single Copy Cluster (SCC) using a shared quorum architecture. This configuration is also available for Exchange Server 2003. We will introduce the new features related to clustering planned for Windows Server codename "Longhorn," and explain which pain points this will fix. You will learn the requirements for setting up a server cluster and find out how to recover from certain cluster specific failures. A virtualized environment will be used to demonstrate the topics discussed.

EXCHANGE BACKUP AND RECOVERY USING VOLUME SHADOW COPY SERVICES
JUERGEN HASSLAUER

Starting with Exchange Server 2003 it was possible to back up and restore Exchange databases using Volume Shadow Copy Services (VSS). Exchange Server 2007 enhanced the support for VSS backup and recovery. You have to use VSS if you want to back up the database copy created by Local Continuous Replication (LCR) or Cluster Continuous Replication (CCR). This topic gets even more interesting with the upcoming release of Microsoft System Center Data Protection Manager (DPM) version 2 by adding support for Exchange backups to DPM. This session provides an overview of the components and their interaction used by an Exchange VSS solution. You will learn what you have to consider during your storage design to meet your service levels. We describe how VSS helps to prevent a backup from disturbing your production Exchange server, and how you can use a shadow copy to recover a corrupt storage group.

EXCHANGE 2007 HIGH AVAILABILITY
SHREE VISHWANATHAN

Well folks, Exchange 2007 is here and with it has brought a new way of thinking while designing for high availability. Continuous replication in Exchange 2007 introduces some new "out of the box" availability options, particularly for the mailbox server role, such as LCR (Local Continuous Replication) and CCR (Cluster Continuous Replication). This session unravels the new features while highlighting factors to consider during the planning and design of Exchange 2007 environments.

CROSS FOREST FEATURES IN EXCHANGE 2007
WENDY FERGUSON

Exchange 2007 brings many new features to support cross-forest environments. In this session, we'll describe those features and give practical best practice guidance on how to plan, design, and implement your multiforest environment.

EXCHANGE 2007 WEB SERVICES
WENDY FERGUSON

Exchange 2007 has a multitude of Web services that radically alter the mechanism by which client applications and programmers can make use of Exchange features and functions. In this session, we'll describe all of the new Web services, what they are, and when they come into play.

TO DO, OR NOT TO DO? MANAGING LARGE MAILBOXES
MISSY KOSLOSKY

Are your end users pack rats? Are YOU a pack rat? What are the actual ramifications of large mailbox sizes in Exchange? We'll discuss size limits for mailboxes, the scalability of Information Stores, and what you should be doing in order to keep your end users and your servers happy!

ACTIVE DIRECTORY SITES AND SERVICES—IT'S NOT JUST FOR ACTIVE DIRECTORY ANYMORE!
MISSY KOSLOSKY

Message transport in Exchange Server 2007 relies on your Active Directory Sites and Services configuration—do you need to revisit the configuration of Active Directory in your organization? We'll talk about the implications of the routing changes in Exchange 2007, and what they might mean to your current configuration.

DIVESTING RESOURCES IN EXCHANGE SERVER
MISSY KOSLOSKY

Your company has sold off a portion of its business—what do you need to do to remove the associated mailbox data from your organization? Let's delve into the ways that we can transfer data from one organization to another while retaining the security of our messaging systems.

EXCHANGE 2007 AND COMPLIANCE
KIERAN MCCORRY

Exchange 2007 allows you to implement various e-mail policies that can help you meet your compliance and records management needs. Similarly, Microsoft Office SharePoint Server 2007 enables you to put much more control on your enterprise document content. Where do all these technologies fit together and how will your users avail of them? In this session, we cover the major advancements in this area highlighting how you can make the best use of these technologies.

BEST PRACTICES FOR DATA PRIVACY WITH YOUR E-MAIL SYSTEM
KIERAN MCCORRY

Everyone knows of the need for system administrators to access mailboxes from time to time to check something out. But are they breaking the law when they do so. The sessions gives an outline of some of the regulations that are relevant when accessing personal data in the US and elsewhere and helps you implement a data access policy to keep you on the right side of the law.

HOW TO GET YOUR END USERS HAPPY WITH LIVE COMMUNICATIONS SERVER 2007
LEE MACKEY

With IM traffic supposedly surpassing e-mail traffic by 2008, how are we as IT Professionals preparing ourselves for this? When end users will install anything and everything to get connected to their kids, significant others, coworkers, and anyone else they want to chat with, how do we tackle this to ensure that we are meeting all requirements from Sarbanes-Oxley, or HIPPA? What tools do we have to ensure that we are following the rules that have been set for us. How do we get clients to communicate over Secure IM from every IM cloud? With Live Communications Server (LCS) 2007, you now have the one-stop-shop. You have the ability to implement a secure communication mechanism that will allow you to get them off the ground and commu-

nicating. With LCS you will have the ability to set up Instant Messenger so your end users will be happy, have the connections they are looking for, and the ability to collaborate with peers, customers, and vendors with little or no effort. In this session we will go over typical deployments, typical policies, extras you might want to consider, and tools to help ensure your end users are just a click away from their buddy list.

MOBILE CLIENT CONNECTIVITY FOR EXCHANGE (ACTIVESYNC)
LEE MACKEY

Microsoft Exchange 2003 with SP2 has become the buzzword in the IT industry. IT Admins no longer need the Blackberry or Goodlink server to get critical data to their end users. Typically with these products the technology requires extra access, more hardware, and sometimes very complicated issues that are nearly impossible to troubleshoot. Microsoft has helped IT Admins with a solution that handles all of these issues. You no longer need extra hardware, or even extra permissions to manage Exchange Server 2003 SP2. This session will walk you through the installation, configuration, and tools to help troubleshoot ActiveSync.

ESSENTIAL TOOLS FOR EXCHANGE ADMINS
LEE MACKEY

Microsoft Exchange 2003 SP2 / 2007 can be very complicated or simple depending on your organization's requirements around e-mail and delivering that service to your end users. In this session, we'll go through a number of tools that will help you troubleshoot and fix issues that you are experiencing, as well as different support options around supporting Exchange. This session will give you details on what to do and how to do it to ensure your success in a critical pinch to get mail flowing again. We don't cover everything, but we will cover the basics and some cool tools and methods for figuring out what's going on.

DCAR WITH EXCHANGE
DEVIN GANGER

Discovery, Compliance, Archival, and Retention: they're challenges every Exchange administrator faces. Whether you're using Exchange 2000, 2003, or 2007, join the author of the *Windows IT Pro* "E-mail Discovery and Compliance" e-book to find out how to solve these challenges.

10 TIPS TO MAKE YOUR EXCHANGE SERVER A GOOD NET NEIGHBOR
DEVIN GANGER

Many Internet mail administrators consider Exchange to be a poorly behaved SMTP MTA. All too often, these perceptions are rooted in configuration errors surrounding Exchange, rather than in any flaw in the product. Learn these common (and in many cases) simple configuration changes you can make that will keep your external mail running smoothly.

IRON CHEF: USING POWERSHELL WITH EXCHANGE 2003
DEVIN GANGER

While the new Exchange Management Shell is only designed to manage Exchange 2007 servers, the underlying PowerShell technology can make managing and scripting your Exchange 2000 and 2003 servers a lot easier. Join one of the authors of the ***Exchange Server Cookbook*** and learn how to take advantage of PowerShell to make scripting Exchange easier than ever.

CONTINUOUS BACKUP FOR EXCHANGE
PAUL ROBICHAUX

Exchange makes full use of both conventional and point-in-time backup technologies. However, many administrators want more! This session will explain the underpinnings of continuous backup solutions from Microsoft and third-party vendors for Exchange 2003 and Exchange 2007 so you can choose an appropriate solution for your needs.

POWERSHELL FOR BEGINNERS
PAUL ROBICHAUX

The Exchange Management Shell (EMS) is a key part of the Exchange 2007 experience. What if you're not a scripter? Don't worry; you can still get plenty done with EMS after just a little learning. This session covers the basics of what you need to know about how EMS works and what you can do with it.

EXCHANGE 2007 UNIFIED MESSAGING DEEP DIVE
PAUL ROBICHAUX

Ever wonder how Exchange 2007 UM does its magic? Come to this session to look under the covers and learn how the UM server, your PBX, and the worldwide phone network work together—in depth.

TROUBLESHOOTING PERFORMANCE ISSUES IN EXCHANGE 2003
WILLIAM LEFKOVICS/KEVIN MILLER

We will outline troubleshooting steps for common performance issues experienced with Exchange 2003, specifically dealing with sluggish performance. We will walk through troubleshooting steps to isolate causes from CPU, disk space, memory, bandwidth and third-party applications. We can also use sysinternals filemon to show I/O distribution.

MESSAGE HYGIENE IN EXCHANGE 2003
WILLIAM LEFKOVICS/KEVIN MILLER

We will review the layered approach administrators can apply to help keep users' inboxes clean of productivity-draining content. We won't waste time on spam statistics. We'll discuss configuring each component and its value to the overall goal.

EXCHANGE 2007 TRANSPORT RULES
WILLIAM LEFKOVICS/KEVIN MILLER

Replacing the cumbersome event sinks, transport rules are easy to administer and resemble a GUI we might see on an e-mail client. We can show how transport rules can make the administrator's job simpler. They are quite granular. We will highlight common ones and ones that might make administrators happiest.

EXCHANGE 2007: THE FIRST 100 DAYS
JIM MCBEE

Follow the real-life implementation of an early adopter of Exchange 2007. This session will start with an overview of the organization's Exchange 2000 architecture and some of their goals for an early implementation of Exchange 2007. The session will then cover the planning process, server consolidation factors, hardware requirements, existing software that integrates with Exchange, and meeting prerequisites. This session will also include many of the hurdles that this organization faced in completing their migration.

ARE YOU A LOW-HANGING FRUIT?
JIM MCBEE

Hackers frequently target the simplest and easiest systems that they can exploit. If common exploits don't work they usually move on. Is your Exchange system vulnerable to "low-hanging fruit" compromise? This session will start by covering simple things you can do with Exchange 2000/2003/2007 to ensure that you are not one of the low-hanging apples on the tree. After covering the basics, we will then cover additional security mechanisms that tools such as Microsoft ISA Server, Edge Transport services, and other tools can provide when implementing additional layers of security and message hygiene.

EXCHANGE 2003: BEST PRACTICES DAY-TO-DAY
JIM MCBEE

What should you be doing on a daily basis to keep your Exchange servers stable and running optimally? Topics in this session include the basic tasks that should be performed on every Exchange 2003 server and events to watch for in the event logs. What can you do to improve your Exchange operations, customize your operations, and tweak Exchange to meet the requirements of your organization? Also covered are some "worst" practices in Exchange management such as "over administering" the Exchange server and common configuration mistakes.

Microsoft EXCHANGE Troubleshooting Course

Hands-on

Sign up for one, two, or all three days of this troubleshooting course. Inside you will learn the issues and methods for troubleshooting and resolving Exchange Server 2003 problems. Each day is packed with in-depth technical information not found in other courses, with Exchange Server 2003 hands-on-labs that walk you through the tools and procedures you'll need when troubleshooting Exchange Server 2003.

You must be registered for the conference to attend the troubleshooting classes. You must indicate when you register, which days you plan to attend.

EXCHANGE TROUBLESHOOTING SPECIALIST COURSE TOPICS INCLUDE:

MONDAY, APRIL 2 — TROUBLESHOOTING DISASTER RECOVERY WITH EXCHANGE SERVER 2003

Covers the Exchange Database Architecture in detail along with the tools and processes used to recover an Exchange Server 2003 environment. In this one-day workshop the student gets hands-on experience recovering from different types of disaster recovery scenarios. **Just Added:** An overview of Exchange Server 2007 Disaster Recovery enhancements.

TUESDAY, APRIL 3 — TROUBLESHOOTING MESSAGE FLOW IN EXCHANGE SERVER 2003

Reviews the Exchange Server 2003 Transport architecture, message flow dependencies, Active Directory (a messaging dependency), troubleshooting tools, DNS issues that affect Mail Flow, Recipient Update Service, and troubleshooting mail flow. **Just Added:** An overview of Exchange Server 2007 message flow.

WEDNESDAY, APRIL 4 — TROUBLESHOOTING PERFORMANCE IN EXCHANGE SERVER 2003

Covers performance monitoring concepts, monitoring performance strategies, and the performance monitoring process. These topics are followed by a review of the tools and how to isolate the performance problem. **Just Added:** An overview of Exchange Server 2007 sizing and tools.

"Very informative session. Lecturer has impeccable knowledge of the subject. This course is extremely useful and relevant to anyone who manages Exchange."

- Vaughn Jardine
THE UNIVERSITY OF THE WEST INDIES

"This is the best courseware, presenter, and labs I've ever attended. And I've been to many. Well done."

-2005 Orlando course attendee

Windows Scripting and Automation Course *Hands-on*

YOU MUST PRE-REGISTER FOR THE VBSCRIPT COURSES.

You will need to bring your own laptop computer with power cord and CD-Rom drive.
See Web site for configuration details.
www.WinConnections.com

You must be registered for the conference to attend the scripting and automation course.

MONDAY, APRIL 2

VBSCRIPT MASTER COURSE

Take VBScript further with scripting guru Don Jones! Learn to utilize databases within your scripts to build more effective and powerful script-based tools. Learn to use the complex WSF format (which Don conveniently de-complicates for you) to build command-line tools by using VBScript—a great way to share your scripts with less experienced technicians. You'll also learn to build a graphical user interface for your scripts using HTML Applications (HTAs). Don rounds out this Master Course with a thorough debugging methodology that will get your scripts up and running faster than ever. Requires attendance at the VBScript Basic Training pre-conference workshop, or equivalent independent experience. This is not an introductory course and assumes prior knowledge of WMI, ADSI, and the VBScript language.

This is a three-part course. You must sign up for Part 1, 2 and 3.

TUESDAY, APRIL 3

POWERSHELL MASTER COURSE

Go beyond the basics and make Windows PowerShell a workhorse for administrative automation and reporting. Scripting guru Don Jones helps you learn complex functionality like how to utilize databases, how to work with regular expressions, and even an introduction to building a graphical user interface from PowerShell's command line. Learn about formatting, sorting, and filtering options that make your PowerShell commands and scripts more effective, and learn best practices for writing effective, maintainable PowerShell code. Requires attendance at the Windows PowerShell Basic Training pre-conference workshop, or equivalent independent experience. This is not an introductory course.

This is a three-part course. You must sign up for Part 1, 2 and 3.

Register Now!
These hands-on classes sell out quickly!

WINDOWS

SESSIONS PRESENTED BY MICROSOFT

Immerse yourself in the latest Windows administrative technologies—**Windows Vista**, **Windows "Longhorn" Server**, **WDS**, **Virtualization**, and more—**with experts from Microsoft Corporation and world-renowned subject matter experts!** Windows Connections offers the deepest and most relevant education for Microsoft Windows administrators, especially in this time of important new products and technologies.

Microsoft is bringing major changes for 2007, and now is the time for you to quickly come up to speed. **Be prepared for the newest technologies and products**, through the real-world experience of our expert presenters and instructors. "Insider" details help you make sense of new technologies, apply them to your environment, and master them faster and more effectively.

- For **Windows Vista**, learn about hidden security truths, volume license activation (a major deployment hurdle if you're not ready), new Group Policy settings, application compatibility issues, and top features that will save you time and money—and that you're likely to overlook!
- For **Windows "Longhorn" Server**, the next generation of Microsoft's server platform, learn what's changed in Active Directory Services, how name resolution has changed, and how File Replication Services have been superseded by DFS-R.
- General **Windows Technologies** changes speed up deployment and re-imagine the way your enterprise works. Learn about Windows Deployment Services, automated provisioning of secure business data shares, how SharePoint will replace your file servers, and how to automate and improve user and group administration.
- This is the year of **virtualization** as hardware and software hypervisor technologies converge. Learn about virtualization strategies for the enterprise, how virtualization can revolutionize your disaster recovery plan, and more.
- Become a more effective and efficient administrator through **scripting and automation**, including powerful tips in VBScript and a comprehensive course in Microsoft's newest automation solution, Windows PowerShell.

IMAGING WINDOWS VISTA

An important component of the new imaging capabilities provided with Windows Vista is the Windows Imaging, or WIM, file format. We will discuss how this new file-based image format provides advantages and capabilities beyond typical sector-based imaging solutions. We will look at how to capture a Windows Vista image, how to view these image files, and edit these files and the configuration settings within the image files themselves using ImageX. Finally, we will look at options for deploying the WIM file. The WIM file is installed differently than previous images and there are new options for deployment within an organization. We are not going to go into detail of the deployment process but will give an overview of how it works and its role in the imaging process.

WINDOWS "LONGHORN" SERVER TECHNICAL OVERVIEW, PART 1

This is part one of a two-part session discussing the features of Windows "Longhorn" Server. In this session, we will look at new features that will enhance productivity and performance. We will discuss new features in IIS and Clustering support. We will also demonstrate using the new Windows PowerShell for administration and the new Performance and Reliability Monitor.

SQL 2005 SECURITY FEATURES

SQL Server 2005 breaks security down into a number of distinct areas. We will be introducing the security concepts that are new to SQL Server 2005, such as user-schema separation. We will also see how SQL Server 2005 implements current security concepts like encryption in ways that are new to this release. The session will look at security from the perspective of the server, the database, and database objects, and some of the different options you can use at each level to help secure your data. The session will also take a look at how you can monitor the security of your SQL Server.

DEPLOYING VISTA WITH BDD 2007

Business Desktop Deployment, or BDD, has changed the face of scaled desktop deployments, providing true end-to-end guidance and automation for all required desktop deployment processes. In this session we will look at how the deployment toolset has changed for operating systems. We will look specifically at how a Windows Vista deployment will be accomplished. We will see how the new WIM image format works and how to design a light-touch or zero-touch deployment of the new operating system. Finally, we will tour and use the new Business Desktop Deployment 2007 Solution Accelerator.

WINDOWS "LONGHORN" SERVER TECHNICAL OVERVIEW, PART 2

In this second part of our overview of Windows "Longhorn" Server, we will provide a brief introduction to Network Access Protection, which will allow administrators to enforce compliance with health policies for network access or communication. Also, Terminal Services has undergone some significant changes and improvements since Windows 2003.

WINDOWS VISTA SECURITY FEATURES

Discover new features in Windows Vista that will help keep the bad stuff out. We will discuss improvements in the Windows Firewall, IE security features, User Account Control, Network Access Protection, and more.

GROUP POLICY IN VISTA

This session will describe the new and updated features in group policy and how these help alleviate problems that were present with previous versions of Windows. With the number of Group Policy settings having increased from approximately 1,700 in Windows Server 2003 with Service Pack 1 to approximately 3,000 in Windows Vista and Windows Server "Longhorn," we will only look at the biggest improvements and give a good starting point for you to utilize the new Group Policy settings. We will also introduce Quality of Service policies which are available with Windows Vista.

NETWORK ACCESS PROTECTION IN WINDOWS "LONGHORN" SERVER

It's not enough to just keep the "bad guys" out of the network anymore. Authorized users and workstations can also contribute security issues behind the firewall. Network Access Protection allows you to check the health of these systems before granting them full success to the network. We will discuss using NAP with IPSec, DHCP, VPN Policies and more.

SECURING THE BRANCH OFFICE WITH ISA 2006

In this session, we well cover the tasks for deploying an ISA solution in a branch office. This will involve configuring both the headquarters and branch office sites, and deploying a site-to-site VPN connection using the layer two tunneling protocol over IPsec, or L2TP. We will explore the new performance-enhancing features that can really make a difference for branch office users, including HTTP compression, content caching, and traffic prioritization using DiffServ. Finally, we will focus on monitoring ISA Servers with MOM 2005 and the ISA Server management pack, including how to deploy the MOM agent to an ISA Server.

WINDOWS VISTA FIREWALL AND ADVANCED SECURITY

In this session, we are going to look at features of firewalls in general and specifically the firewall included with Windows operating systems. We will be using some of the features in previous versions of Windows Firewall to highlight the new benefits of the Windows Firewall with Windows Vista. Vista provides greater configuration options resulting in greater security for different connection methods, such as LAN or wireless connections. We will look at ways to configure exceptions for more control over incoming and outgoing traffic.

UNIX INTEROPERABILITY IN WINDOWS "LONGHORN"

We live in an increasing integrated world where Windows servers must play in the same sandbox with many other operating systems. In this session, we will discuss interoperability improvements in Windows "Longhorn" server that allow Windows and Unix-based systems to live together in better harmony.

WHAT IS FOREFRONT AND HOW WILL IT HELP ME?

Today's security market landscape is complex and fragmented. Poor interoperability, separate management consoles for each product, and a general lack of unified event reporting and analysis all present challenges to the system administrator. Learn how the Forefront family of products can protect your network and systems including client workstations, Exchange, SharePoint, ISA, and Office Communications Server.

NEXT GENERATION NETWORKING IN WINDOWS VISTA AND WINDOWS "LONGHORN" SERVER

The Next Generation TCP/IP stack in Windows Vista and Windows Server "Longhorn" is a complete redesign of TCP/IP functionality for both Internet Protocol version 4 (IPv4) and Internet Protocol version 6 (IPv6) that meets the connectivity and performance needs of today's varied networking environments and technologies. The Next Generation TCP/IP stack introduces many security, performance, and scalability improvements. After we've examined the new features and benefits of the Next Generation TCP/IP stack we'll discuss how you can prepare your network for IPv6.

WINDOWS DEPLOYMENT SERVICES TECHNICAL OVERVIEW

In this session, we will look at how WDS takes advantage of the Windows Imaging, or WIM, file format. WDS is actually made up of several components to form a unified deployment solution. We will explore each of these components to see how they interact. The management component of WDS is simplified to provide an easy solution for administrators; we will show how using the simplified management with WDS will allow companies to reap these benefits.

IDENTITY AND ACCESS MANAGEMENT

As organizations grow, they tend to accumulate multiple systems and standards for storing, managing, and using digital identities. These systems can include directory services, human resource (HR) databases, financial systems, and custom applications, in addition to Web sites for employees, customers, and partners. The complexities that result from having multiple identity systems and standards generate higher costs, management overhead, and security issues that grow as the size of the environment increases. Implementing an identity and access management solution can help organizations take control of their environments and reduce the complexity.

SESSIONS AND SPEAKERS
ARE SUBJECT TO CHANGE.
SEE WEB SITE FOR UPDATES
AND ADDITIONAL SESSIONS.

WINDOWS
CONFERENCE SESSIONS

WHAT'S NEW IN DIRECTORY SERVICES FOR LONGHORN SERVER?
SEAN DEUBY

A lot of work has been done on Active Directory for Longhorn Server with features that give you more flexibility in your directory than you've ever had. In this session, you'll learn about better security for DCs in insecure locations, improved ways to promote and demote DCs, and finally the ability to safely grant administrator rights to operators on some DCs. It is time to start thinking toward your Longhorn future!

IDENTITY MANAGEMENT FUNDAMENTALS
JAN DECLERCQ

This session provides an extensive introduction to identity management. It explains the concept of a digital identity and how it can be used in different contexts. The session pays special attention to the identity management components in the data repository, security, lifecycle, consumable value and management areas. It also introduces identity management-related standards and looks at what solutions Microsoft can offer in this space.

NEW FEATURES IN PKI AND CERTIFICATES FOR LONGHORN AND VISTA
BRIAN KOMAR

Brian Komar, one of the leading "gurus" in Public Key Infrastructure, shares his insights into the changes to PKI and Certificates in Windows Vista and Windows "Longhorn" Server. Learn what you need to know to prepare to implement these technologies, and what they mean to your business.

NETWORK ACCESS PROTECTION IN WINDOWS VISTA AND LONGHORN
STEVE RILEY

Many organizations wish to limit access from and prevent damaged caused by rogue, unmanaged machines. This is a challenge because the underlying network protocols were designed primarily to facilitate ease of communications, not to provide robust authentication or permission checking. Many products are becoming available to help control access into a network, based on a variety of existing technologies: DHCP, 802.1X, and IPsec are the most popular. Steve Riley will explore Microsoft's Network Access Protection (NAP) offering, included as part of Windows Vista and Windows "Longhorn" Server.

REIMAGINING THE FILE SHARE: AUTOMATING AND PROVISIONING SECURE BUSINESS DATA SHARES
DAN HOLME

Whether for security, compliance, or manageability, the time has come for IT organizations to reexamine how they manage traditional file shares. This practical, solutions-focused session will present a vision for role-based, provisioned management of shared data folders. You will take away tools and a punch-list of processes that you can adapt to your enterprise's requirements to achieve that vision. Participants in this session are expected to have a solid understanding of access control lists (ACLs) and group management in Active Directory.

DEPLOYING AND MANAGING SMART CARDS WITH CERTIFICATE LIFECYCLE MANAGER
BRIAN KOMAR

Certificate Lifecycle Manger (CLM) allows you to manage software and smart card certificates in your network through the lifetime of the certificates. This session provides an overview of the product, how it integrates into your existing PKI, and identifies how the product will help you in your future certificate deployments.

WINDOWS VISTA SECURITY: THE HIDDEN TRUTH
MARK MINASI

Vista's more than just a pretty face. Its security innards have been ripped out and replaced with a new and almost completely different security engine. But it's not just security geek internals, friends: it's some whole new paradigms. For example, what's going on with those User Access Control dialog boxes behind the scenes? Think you know what's in a SID? Not any more… and get ready for a whole new layer of security, the Mandatory Integrity Controls. MIC's the thing that could make it nearly impossible for you to delete any file in System32, even if you're an administrator. Ah, have we got your attention now? Then don't miss this session!

COMMON ACTIVE DIRECTORY ATTACKS AND HOW TO PROTECT AGAINST THEM
JAN DECLERCQ

This session provides examples of common attacks against Active Directory and also shows how you can protect your enterprise directory against them. The attacks addressed in this presentation include password cracking-, elevation of privilege- and denial-of-service-based attacks.

EVERYTHING NEW IN VISTA AND SERVER EVENTS AND EVENT LOGS
RHONDA LAYFIELD

Join Rhonda Layfield for an in-depth look at the overhauled event logs and eventing subsystems of Vista and Longhorn. Learn how to navigate the logs, consolidate, locate, and interpret events.

WINDOWS VISTA FIREWALL WITH ADVANCED SECURITY: A DEEP-DIVE
DOUG SPINDLER

Administrators may be familiar with the basic firewall found in Vista, which is very similar to the firewall found in Windows XP. In Vista, IT Pros will discover that Microsoft enhanced the functionality of the basic firewall with Windows Firewall with Advanced Security. The Advanced Security Firewall will allow IT Admins to have much more control over firewall settings such as source and destination IP addresses, IP protocol number, source and destination Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) ports, interface types, Internet Control Message Protocol (ICMP), and ICMP for IPv6 (ICMPv6). The new advanced security firewall in Vista offers a new level of security and functionality in Vista including the ability to filter inbound and outbound traffic. The new firewall is just one more reason why you will want your users using Vista.

THE FILE SERVER IS DEAD: IMPLEMENTING WINDOWS SHAREPOINT SERVICES DOCUMENT LIBRARIES
DAN HOLME

After a short life of barely a decade, the Windows Server shared folder is dead, or at least on life support. Why? Because the features that we've all been missing—version control, version history, extensibility, and workflow—are now achievable using Windows SharePoint Services document libraries. Learn how to move forward into a new era of document management in this practical introduction to WSS.

DISTRIBUTING YOUR DATA WITH DFS NAMESPACES
SEAN DEUBY

DFS Namespaces is one of the greatest features in Windows Server that's not widely known. A significant improvement over the original Distributed File System in Windows 2000, learn how to use DFS Namespaces to quickly and easily build, manage, and delegate an easy-to-use enterprise virtual folder structure.

MOVING TO 64-BIT WINDOWS
GUIDO GRILLENMEIER

2006 is the year in which 64-bit computing has gone mainstream and its adoption will continue

to grow at fast pace in 2007. The availability of a powerful x64 processor architecture that is backward compatible with the prevailing x86 architecture and the availability of Windows Server x64 editions that leverage this architecture allow a smooth migration path for customers into the new 64-bit world of computing. This session describes the most important things to know about 64-bit and the related Windows Server 2003 and Longhorn operating system versions. It differentiates the two 64-bit architectures supported by Windows (x64 and Itanium) and describes appropriate business cases for leveraging 64-bit today. Special focus will be put on 32-bit compatibility challenges and solutions as well as discussing deployment scenarios for the Windows 64-bit versions and the support of well known server applications when executed on a Windows x64 server operating system.

NAME RESOLUTION 2008 STYLE: DNS, WINS, AND NETBIOS IN LONGHORN

MARK MINASI

Soon we'll have "NT Server 6.1" —Vista's big brother, also known as Server 2007, 2008, or Longhorn. And with that comes improvements in, well, just about everything, including one of Windows' most important pieces of plumbing—name resolution. Yes, you've heard it before, but with Longhorn, it looks as though WINS may really, finally, actually... die. Or not; we'll see. Besides the changes to WINS, the big name resolution story is, of course, DNS. What's new in 2007/8 DNS? And, better, what small features of 2003's DNS might you be missing out on? Come to this session with The Master of Name Resolution, popular speaker and writer Mark Minasi, to find out!

UNDERSTANDING AND TROUBLESHOOTING WINDOWS SERVER 2003 AUTHENTICATION

JAN DECLERCQ

This session focuses on the nuts and bolts of the Kerberos authentication protocol: the basic protocol exchanges, the protocol's strengths and its operation in a single- and multidomain and multiforest environment. The session also addresses the new key features of the Kerberos implementation in Windows Server 2003 and R2: these include the support for protocol transition, constrained delegation, and user-to-user authentication.

DFS-R: THE GOOD, THE BAD, AND THE NON-REPLICATED

RHONDA LAYFIELD

Windows Server 2003 delivers a new mechanism for replicating data in DFS Namespaces called DFS-Replication or DFS-R. DFS Namespaces are incredibly easy to set up and they seem to just magically replicate from one server to another. But what happens when the magic wears off or when replication fails? In this session, you will learn how to monitor and troubleshoot the new DFS-R to keep the magic alive in your enterprise. Rhonda will share useful command-line tools that configure the client to fail-over to a specific server. She will also dig deep into the replication mechanism to expose the inner workings of cross-file RDC. You'll discover how DFS-R determines what has changed in a file and replicates only the changes—not the entire file—conserving network bandwidth utilization.

CHANGES IN DELEGATING ACTIVE DIRECTORY IN LONGHORN

GUIDO GRILLENMEIER

Active Directory enables administrators to assign permissions to all directory objects at a very granular level. Enterprise environments need to leverage this capability to differentiate who can see or do what in which part of their directories. However, the granularity of permissions in Active Directory can be hugely overwhelming and needs to be applied and managed correctly. This session will recap the challenges of delegating administrative permissions in AD and describe the upcoming changes in Longhorn Security as they are relevant for AD delegation. It will cover typical scenarios for management of Active Directory objects in large enterprises, answering such critical questions as: How can I differentiate between admins that can create objects and those that can manage or delete them? How do I best manage the new options to separate the admin role on Read-Only-DCs? It will also highlight and explain many of the not-so-well-known features around AD delegation that are lingering in your Windows Server 2003 AD infrastructures.

WHAT'S NEW IN WINDOWS VISTA GROUP POLICY?

JEREMY MOSKOWITZ

Short answer: lots. So come hear the essental "what every admin absolutely needs to know" about Windows Vista and Group Policy. Learn why you need a Windows Vista management station. Learn how to get out of burning 5MB per GPO on each DC. Learn about the new things you can do (like power management and USB port management)—only for Windows Vista clients. If you've got even one Windows Vista client that you're going to deploy, you positively must come to this session to learn the ropes from Jeremy Moskowitz, Group Policy MVP.

FRS RIP: DFS-R REPLICATION AND SYSVOL IN WINDOWS SERVER

RHONDA LAYFIELD

Longhorn Server will use DFS-R to replicate your sysvol data. If you have ever had the need to troubleshoot a sysvol replication failure—maybe a group policy object which dictates your clients security settings failed to replicate to one specific domain controller, so the clients in that site do not receive the security settings; then you know the joys of troubleshooting sysvol replication. Learning the step-by-step process DFS-R uses in the replication process will be a huge help. This session is an in-depth look at DFS-R and the known issues you may possibly run into. This session also contains information that is not yet documented. Learn the process now and be one step ahead of any issues you may encounter!

VIRTUALIZATION STRATEGIES AND TECHNOLOGIES FOR THE ENTERPRISE

ALAN SUGANO

Server and application virtualization in the enterprise environment continues to rise in popularity. As server hardware becomes more powerful, much of the processing power of the server is wasted. Server virtualization allows you to efficiently use the processing power of new servers and the 64-bit platform by consolidating multiple physical servers onto a single virtual server host. We'll examine ESX Server and Microsoft's Hypervisor technologies and how they work with server virtualization. Application virtualization allows you to run applications on workstations without having to install the application on each workstation. This simplifies patch management and significantly reduces the time to roll out new or upgraded applications. Virtualization has the potential to save money, reduce server setup time, provide a flexible test environment, speed up disaster recovery, and still provide high availability.

GOODBYE RIS, HELLO WDS

JEREMY MOSKOWITZ

RIS is dead. Long live, RIS, er, WDS, which replaces RIS. What was RIS? An in-the-box way to deploy scripted, hands-off installs for Windows XP and Windows 2003. What's WDS? The all-new, in-the-box way to deploy scripted, hands-off installs for Windows Vista, Windows XP, and Windows 2003. If you're using RIS today, you absolutely MUST come to this session to know how to upgrade your RIS servers. If you're flirting with Vista installation, learn one unified way to zap out Windows Vista and Windows XP.

REIMAGINING THE MOBILITY AND AGILITY OF USER DATA: FOLDER REDIRECTION, ROAMING PROFILES, AND OFFLINE FILES

DAN HOLME

Windows Server 2003, Vista, and XP offer important functionality to ensure that data is available and secure. But until you start managing the intricacies of the technologies, your organiza-

tion's data is difficult to access or take offline, challenging to protect, and intellectual property is exposed. In a worst-case scenario, critical user data is stored only on users' machines and is exposed to complete loss. Or, misguided corporate mandates lead too quickly to full-disk encryption. In this practical session, you will learn best practices for putting the pieces together: folder redirection, user profiles, offline files, encryption, Group Policy, ACLs, and shares. Participants are expected to have a very solid understanding of most or all of these technologies, or be ready to learn them offline. This advanced session prepares you to take away ready-to-implement, useful solutions to corralling, securing, and managing corporate data.

APPLICATION VIRTUALIZATION

ALAN SUGANO

End the patch management hell. Application virtualization allows you to run applications without having to install the application on each workstation. This simplifies patch management and significantly reduces the time to roll out new or upgraded applications, because patches are installed once on the application server and not individually on each workstation. We'll take a look at Microsoft's Softricity technology and how it handles local, remote, and disconnected clients and their applications. This technology also leads to the software as a service directive that many companies see as an industry trend. Application virtualization also ties into disaster recovery because it significantly reduces the prep time for workstation recovery. Application virtualization can reduce patch management headaches, reduce the time to roll out new applications, easy roll back for problematic patches, allows users to run different versions of the same application, and can speed up disaster recovery. See if this technology is a good fit for your company.

DEBUNKING SECURITY MYTHS 2007

STEVE RILEY

Let's see now, if we just tweak this setting here and that setting over there and the other setting … um, where was that setting again? Sounds familiar, huh? Security tweaks often make you feel good because, after all, you've done something! Alas, tweaks are usually nothing more than pure "security theater," designed more to satisfy poorly written auditing requirements than really making a system more difficult to attack. Steve Riley will expose several common security myths and explain why they provide little (if any) value.

SESSIONS AND SPEAKERS ARE SUBJECT TO CHANGE. SEE WEB SITE FOR UPDATES AND ADDITIONAL SESSIONS.

VOLUME ACTIVATION 2.0 IN VISTA AND LONGHORN SERVER

SEAN DEUBY

Think you finally understand Windows licensing? Think again! Every single Vista and Longhorn system requires a Volume Activation infrastructure or they'll come grinding to a halt after you've deployed them. Designing for VA 2.0 will be a critical part of your Vista/Longhorn deployment, so check out this session and be prepared.

IMPACT OF EXCHANGE 2007 ON YOUR ACTIVE DIRECTORY

GUIDO GRILLENMEIER

Exchange 2007 is one of those applications that will have quite an impact on your Windows infrastructure once you choose to deploy it. This includes the fact that the deployment of Exchange will force you to implement 64-bit versions of the Windows OS. It will also introduce changes to your Active Directory, including how you delegate the management of messaging-related attributes and how you configure your AD Site Topology. And while there is no immediate dependency to update your Active Directory Domain Controllers to 64-bit Windows as well, various features of Exchange 2007 will have quite an impact on the amount of data stored per user in your Active Directory. So should you upgrade your AD DCs to 64-bit after all? This session will answer this and other questions by describing how the different features in Exchange 2007 could impact your Active Directory.

CRACKING THE DAVISTA CODE: THE BEST THINGS YOU'RE NOT USING IN VISTA

MARK MINASI

So you got yourself some powerful PCs and you put Vista on your desktop. Pretty neat, eh? But it might be neater, you know. After all, Vista's basically a complete re-write of Windows. So while everyone's focused on Aero Glass or previous versions, it's easy to miss some of the not-so-obvious but useful things in the latest version of Windows—things like takeown, icacls, or Vista's ability to resize already-formatted partitions without having to reformat them, to name just a few. Join Mark Minasi, author of ***Administering Vista Security: the Big Surprises*** and ***Mastering Windows Vista Business***, in his quest to squeeze the last bit of neat new functionality out of Vista, while perhaps getting a few laughs in the process!

APPLICATION COMPATIBILITY FOR WINDOWS VISTA

JEREMY MOSKOWITZ

You've got Vista and now you've got problems. Why? Because you've got applications which work TODAY in XP, but maybe not so much in Vista. What are you going to do? We'll start off with the Application Compatibility Toolkit (which does a lot more than you might think) and show you some tips and tricks to make the applications you already have work better in Vista.

SERVER HIGH AVAILABILITY TECHNOLOGIES

ALAN SUGANO

This session will explore high availability solutions from Microsoft and third-party vendors. We will examine lower-end solutions like SQL Server Log Shipping and Database Mirroring that are included with SQL Server 2005, server mirroring from third-party vendors like Neverfail and Doubletake, Microsoft's Server Cluster Solution, SAN options, and how to leverage virtualization technologies, such as VMWare's ESX Server with VMotion, as options for high-availability. The discussion will prepare you to determine which high availability solution is the best fit for your company based on your budget and uptime requirements.

WINDOWS SERVER UPDATE SERVICES 3.0

DOUG SPINDLER

Patch management has kept many an IT Professional busy over the years. Keeping a machine patched and up to date is probably one of the least rewarding tasks for an IT Professional. Several years ago, Microsoft released a free patch management server, but few IT Pros actually implemented it. The Patch Management Server or Windows Server Update Services (WSUS) is now on version 3. There is no reason not to have WSUS running where you work. In this session, we are going to show you step-by-step how to install a WSUS server first without Active Directory, and then with Active Directory. Everyone who attends this session will leave knowing how to set up and deploy a WSUS server.

FILE AND DISK ENCRYPTION WITH EFS AND BITLOCKER

BRIAN KOMAR

Plug potential data "leaks" by encrypting user systems. Explore the pros and cons of Encrypting File System (EFS) and Windows Vista Bitlocker during this practical, technical session.

Microsoft Office 2007:
Deployment Strategies and Techniques

The new Microsoft information worker platform is here: Microsoft Office 2007. Far more than just new versions of Word and Excel, Office 2007 is the new groupware client, information worker portal, and collaboration platform for Microsoft technologies. Leveraging server technologies in Windows, Exchange Server, and SharePoint Server, and based upon the advanced client platform technologies in Windows Vista, Office 2007 is simply a must-have new suite. Are you ready for it?

Rely on Office Connections' expert presenters to share inside tips and tricks, and their deep, thorough experience to make Office 2007 deployments easier, more efficient, safer, and more effective. Learn what makes Office 2007 tick, and learn about the features your users will be relying on to do their jobs—and learn how to deliver those features in an effective, enterprise-friendly fashion.

MIGRATING TO SHAREPOINT SERVER 2007

In this session we are going to look at the upgrade and migration process of the new Office SharePoint Server 2007 in conjunction with the newest version of Windows SharePoint Services. Once you have decided to upgrade, you have several options of how to carry out the upgrade process. We are going to explain these upgrade alternatives, along with the advantages and disadvantages of each choice. With each upgrade approach comes additional considerations. This includes how to handle customizations and how to address the upgrade if you use shared services. We are going to address these concerns and give possible solutions. In addition, we will give tips for pre-upgrade and post-upgrade steps and best practices.

SESSIONS AND SPEAKERS ARE SUBJECT TO CHANGE.
SEE WEB SITE FOR UPDATES AND ADDITIONAL SESSIONS.

PLANNING FOR AND DEPLOYING SPS 2007

We will introduce the three-tier administration model: central administration, shared services, and site settings. Each component will be explained as well as some common usages. We will also explain various security topics including permissions. Finally, we will look at the deployment options. We will provide some considerations for determining the correct topology to use. We will use scenarios to go into detail of four different topologies. The simplest of these is a single server deployment, and then the options progress to farm options, from small to large.

NEW TOOLS AND TECHNIQUES FOR DEPLOYING THE OFFICE 2007 SYSTEM

The 2007 release of the Microsoft Office System offers several new tools to speed and simplify the client deployment process. In this session, you are introduced to the new Setup and Customization technologies (only one tool now instead of all those wizards!) in addition to the new Office Multilingual architecture. This presentation offers a drill down of each tool, guidance for their use, and suggestions for making your deployment a success.

SECURITY AND SHAREPOINT: FROM SERVICE ACCOUNTS TO ITEM-LEVEL ACCESS

In this session we are going to discuss the security methods for Windows SharePoint Services 3.0 and Office SharePoint Server 2007. We will go over different authentication methods, as well as benefits and limitations with these authentication methods. We will discuss the management of permissions and their role with SharePoint groups. We will go over the different permission levels and new permissions available with SharePoint 2007. We will also review access rights that can be used with the SharePoint server. We will discuss the configuration of a Web Farm and review the Web Farm topology, secure topology, secure communication, and security hardening.

WHAT'S NEW IN THE MICROSOFT OFFICE 2007 SYSTEM? CLIENT FEATURE WALKTHROUGH

The innovations in the 2007 Microsoft Office System client applications are significant and range across every aspect of the programs. This session provides an intense high-level tour of these major areas of innovation, including: (1) demonstrations of the most important new capabilities in each of the client applications, (2) insights into migration and coexistence with the new Microsoft Office Open XML file formats, (3) examples of client integration with the new Office SharePoint Server 2007, and (4) a fast-paced overview of the new streamlined Microsoft Office User Interface.

CONFERENCE SESSIONS OFFICE

INTRODUCTION TO KNOWLEDGE NETWORK

DOUGLAS RYAN VANBENTHUYSEN

Learn how Knowledge Network (KN) is positioned within the world of social and professional networking. This session will review basic KN functionality, examine how to address privacy concerns, and suggest some advanced KN uses.

WHAT'S NEW IN ACCESS 2007?

ALISON BALTER

Access 2007 includes a plethora of new features. This session provides the attendee with a tour of Access 2007. The tour will begin with an exploration of the many new form and report features that facilitate the rapid development of new and existing forms and reports. Other topics covered in this session include what's new with tables, the new and improved embedded macros, and what's new with importing and exporting. After attending this session you will be compelled to include Access 2007 as both an end-user and developer tool within your organization.

CONTENT TYPES IN SHAREPOINT

DOUGLAS RYAN VANBENTHUYSEN

Explore the new SharePoint content type feature. This session will explain the value of content types and show how to create and associate multiple content types with a single document library.

BUILDING INFOPATH FORMS THAT RUN AS BOTH RICH CLIENT AND BROWSER APPLICATIONS

DAVID GERHARDT

Examine the new support for server forms in Office InfoPath 2007. This session will review new InfoPath features but will focus on the "design once" concept, which allows for a single form template to be used for both rich-client and browser applications.

OFFICE
CONFERENCE SESSIONS

WHAT'S NEW IN ACCESS 2007 SECURITY?
ALISON BALTER

Access 2007 security is extremely different than that of its predecessors. For example, Access 2007 security eliminates user-level security. These changes to security have major implications on the applications that employees in the organization build. This session covers new topics such as using an Access 2007 database in a trusted location, packaging, signing, and distributing an Access 2007 database, and encrypting an Access 2007 database. It also covers how security works with databases created in other versions of Access. Finally, it covers the process of running unsafe expressions. All of these topics are vital for securing and successfully working with an Access 2007 database.

USING SHAREPOINT DESIGNER AS A WORKFLOW TOOL
DOUGLAS RYAN VANBENTHUYSEN

Examine the workflow capabilities of Office SharePoint Designer 2007. This session will explore the conditional logic that you can build with SharePoint Designer workflows and review the actions that can be performed against SharePoint list items.

GROOVE 2007: GETTING PEOPLE TO WORK TOGETHER
DOUG SPINDLER

Have you ever worked as a team member in a workgroup in which documents were e-mailed to the members of the team for review? If so you will quickly realize that tracking all of the changes and knowing which team member has the most up-to-date document is quite confusing. This is where Groove fits in. In this session, we will take a look at real-world solutions where we have used Groove Service and Groove Server to provide document management solutions for team members from company workgroups. We will show you how large corporations are using Groove Server and how mid-size law firms, advertising agencies, and non-profits are using Groove Service to work together on projects.

LEVERAGING ONE OF SHAREPOINT'S FORGOTTEN GEMS, PART ONE: HARNESS THE POWER OF CUSTOM LISTS
CA CALLAHAN

WSS is often simply written off as a document sharing tool. But *au contraire*, it can be much more than that. Come see how to unlock the hidden database potential of WSS, creating custom lists that allow you to enable your users to access, enter, and display shared data (like inventory, sales, and more). Watch how WSS can become a data management tool with built-in security capabilities, reporting, and more.

LEVERAGING ONE OF SHAREPOINT'S FORGOTTEN GEMS, PART TWO: HARNESS THE REPORTING POWER OF CUSTOM VIEWS
CA CALLAHAN

Every list, table, or database is simply comprised of records of data. And although that's nice, on its own it's not that nifty. It's not enough to simply add data, and it's not enough to simply have it stored somewhere. You have to be able to see it, to query it, to "use" it. And that's what SharePoint lists and their views are all about. Come see how to use the power of view customization and learn a whole new way of using SharePoint.

LEVERAGING ONE OF SHAREPOINT'S FORGOTTEN GEMS, PART THREE: HARNESS THE POWER OF THE SIMPLE, BUILT-IN, LIST VIEW WEB PARTS
CA CALLAHAN

Web Parts are usually considered for developers only, but that's just not true. Come see the third and final installment of the forgotten gems series, and learn how to use Web Parts to your advantage. Don't just fill your home page with stock market tickers and sports stats; learn how to leverage custom lists and their views to make your site's home page more relevant and useful (without becoming a developer).

END-TO-END SOLUTIONS WITH THE 2007 RELEASE: DEVELOPING FOR IT PROS
DAVID GERHARDT

Review an end-to-end solution for a sample building permit application process. This session will show how Office InfoPath 2007 and Office SharePoint Designer 2007 were used together to build a solution that needed only a minimal amount of custom code.

FRONT-ENDING SHAREPOINT WITH ACCESS
ALISON BALTER

Access 2007 is tightly integrated with SharePoint. This session provides the attendee with everything that they need to know about working with Access 2007 and SharePoint. Topics covered include why SharePoint and Access 2007 are important tools within the organization, how to move your database to a SharePoint site, and how to open and work with SharePoint lists from within Access 2007. It will also cover how to integrate with the SharePoint workflow, how to work with SharePoint services offline, and how to map Access data to SharePoint data. All of these topics are necessary when integrating Access 2007 and SharePoint.

TEMPLATES AND CUSTOM STYLES WITH OFFICE WORD 2007
DOUGLAS RYAN VANBENTHUYSEN

Explore the use of custom styles in an Office Word 2007 template, including the interaction between themes, templates, and styles. You will learn convenient ways of applying styles, which includes assigning keyboard shortcuts, placing styles in the ribbon, and applying custom styles to custom themes.

SHARING INFORMATION WITH MICROSOFT OFFICE EXCEL AND EXCEL SERVICES 2007
BOB MIXON

Excel Services, provided by Microsoft Office SharePoint Server 2007, gives users the ability to publish and share Excel workbooks in a central location. Once published, a user can access all or part of those workbooks through their browser using Microsoft Office Excel Web Access. In this session, I will demonstrate how to publish Excel workbooks to Excel Services and utilize various features such as, limiting what sheets and/or cell ranges will be displayed. In addition, I will demonstrate how to use browser-based parameters, giving users the ability to plug in specific cell data.

MICROSOFT OFFICE FORMS SERVER 2007: DELIVERING FORMS WITHOUT CODE
BOB MIXON

In the past, delivering complex browser-based forms to our customers required the experience of an ASP.NET developer. With the combined features of Microsoft Office InfoPath 2007 and Microsoft Office Forms Server 2007, many of these efforts can be pushed out to the line of business. This session will demonstrate the ease of implementing browser-based forms that have rich features such as field-level validation—all without writing a single line of code. In addition, I will demonstrate the means by which these forms can be integrated with Microsoft Office SharePoint for data storage.

SESSIONS AND SPEAKERS ARE SUBJECT TO CHANGE. SEE WEB SITE FOR UPDATES AND ADDITIONAL SESSIONS.

SPEAKERS
MICROSOFT AND INDUSTRY EXPERTS

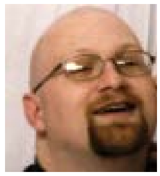
SPEAKERS ARE SUBJECT TO CHANGE. SEE WEB SITE FOR UPDATES AND BIOS.

ALISON BALTER
INFO TECHNOLOGY PARTNERS

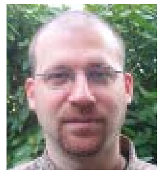
CA CALLAHAN
CALLAHANTECH

JEAN DECLERCQ
HP

SEAN DEUBY
INTEL



DEVIN GANGER
3SHARP



DAVID GERHARDT
3SHARP

GUIDO GRILLENMEIER
HP

JUERGEN HASSLAUER
HP

DAN HOLME
INTELLIEM

DON JONES
SCRIPTINGANSWERS.COM

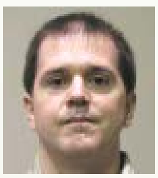
BRIAN KOMAR
IDENTIT

MISSY KOSLOSKY
HP

KEVIN LAAHS
HP
MICROSOFT EXCHANGE CONNECTIONS CONFERENCE CO-CHAIR

RHONDA LAYFIELD
CONSULTANT/TRAINER

LEE MACKEY
ZENPRISE

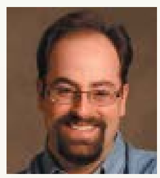


JIM MCBEE
ITCS HAWAII

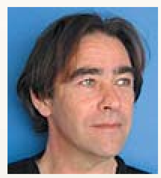
KIERAN MCCORRY
HP
MICROSOFT EXCHANGE CONNECTIONS CONFERENCE CO-CHAIR

MARK MINASI
MR&D

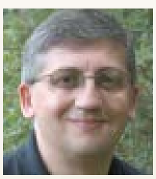
BOB MIXON
MICROSOFT



JEREMY MOSKOWITZ
MOSKOWITZ INC.



PETER O'DOWD
BLADE/WADEWARE



TONY REDMOND
HP

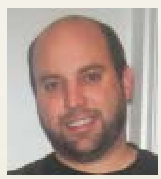
LARRY RIBA
HP

STEVE RILEY
MICROSOFT

PAUL ROBICHAUX
3SHARP
MICROSOFT EXCHANGE CONNECTIONS CONFERENCE CO-CHAIR

DOUGLAS SPINDLER
PACIFIC IT PROFESSIONALS

ALAN SUGANO
ADS CONSULTING GROUP



DOUGLAS RYAN VANBENTHUYSEN
3SHARP

SHREE VISHWANATHAN
HP

ADDITIONAL SPEAKERS INCLUDE:

ENZO FEDRIZZI MICROSOFT
MICROSOFT EXCHANGE CONNECTIONS CONFERENCE CO-CHAIR
WENDY FERGUSON
STAN FOSTER HP
WILLIAM LEFKOVICS MICROSOFT
KEVIN MILLER MICROSOFT

Check our Web site as we add more Microsoft and industry expert speakers.
www.WinConnections.com

WORKSHOPS
PRE-CONFERENCE WORKSHOPS

Pre- and Post-Conference Sessions Boost Your Expertise!

Pre-Conference Workshops:
Sunday, April 1, 2007

Post-Conference Workshops:
Thursday, April 5, 2007

Windows Connections and Exchange Connections offers additional, optional pre- and post-conference half-day sessions. Extend your educational experience and gain additional expertise, including fundamentals that make the main-track sessions more relevant and comprehensible for newcomers.

Pre- and post-conference session selections are available when you register.

SESSIONS AND SPEAKERS ARE SUBJECT TO CHANGE. SEE WEB SITE FOR UPDATES AND ADDITIONAL SESSIONS.

9AM - 4PM • PRE-CONFERENCE WORKSHOP • EXCHANGE TRACK

EPR301: MICROSOFT EXCHANGE SERVER 2007 HANDS-ON LABS

PETER O'DOWD

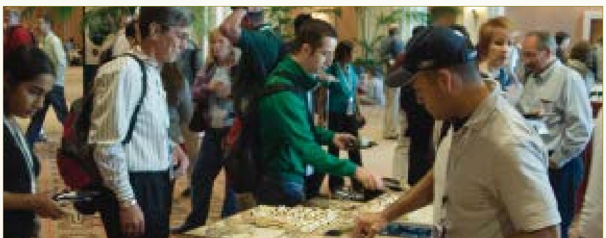
Come take a six-hour guided tour of Exchange Server 2007 and see for yourself the next evolution of the world's most powerful messaging system. Experience the new Management Console, the five new server roles, e-mail policy enforcement and compliance, powerful new scripting tool, new architecture, new high availability and disaster recovery features, new mailbox features, and methods for migrating from earlier versions of Exchange. Sign up fast, seating is limited.

9AM - 4PM • PRE-CONFERENCE WORKSHOP • WINDOWS TRACK

WPR201: REIMAGINING THE IMAGE: DEPLOYING, REPAIRING, REPLACING, AND UPDATING WINDOWS XP AND WINDOWS VISTA CLIENT

DAN HOLME

In this fast-paced, intermediate to advanced session, Dan will share with you best practices and real-world insight into the design, deployment, and maintenance of Windows XP and Vista clients. You will learn new, 21st century approaches to creating perfect (and perfectly supportable) corporate and divisional desktop and laptop images that can be supported effectively with application, security patch, and service pack rollouts into the future. You will take away a deployment methodology that works, and a solid understanding of its functionality so that you can further refine the methodology to apply to your enterprise. Once you leverage the new capabilities of XP, Vista, and Windows Server, your enterprise will be able to roll out and troubleshoot systems faster and more confidently than ever before. Some of Dan's clients have cut out the



CONNECTIONS PARTY

Tuesday, April 3, 2007
BBQ
CASINO GAMES

Subject to weather conditions.

HARLEY-DAVIDSON GIVEAWAY

Enter to WIN

Enter the contest in the Expo Hall to **WIN a Harley-Davidson!** The winner will drive one home.

costs of vendor-installed images after learning how to better manage image creation and deployment internally.

Topics will include Remote Installation Services, Windows Deployment Services, ImageX, Windows PE, and powerful methods for scripted deployment of the operating system and applications (including Microsoft Office). Participants should have familiarity with deployment technologies such as unattended answer files, Group Policy, Sysprep, and disk duplication.

9AM - 12PM • PRE-CONFERENCE WORKSHOP • WINDOWS TRACK

WPR202: VBSCRIPT BASIC TRAINING

DON JONES

A crash course in administering Windows with VBScript! Think VBScript is dead? Think again: Even Microsoft is using it in Windows Server 2007/2008; for many jobs, VBScript is still the right tool. Scripting guru Don Jones, author of ***Managing Windows with VBScript and WMI*** and co-author of ***Advanced VBScript for Windows Administrators***, teaches you everything you need to know about VBScript, Windows Management Instrumentation (WMI), and Active Directory Services Interface (ADSI)—with no prior experience required. You'll even learn Don's tips and tricks for scripting faster and more effectively, including great tips on debugging and bug prevention.

1PM - 4PM • PRE-CONFERENCE WORKSHOP • WINDOWS TRACK

WPR203: WINDOWS POWERSHELL BASIC TRAINING

DON JONES

Learn the basics of Microsoft's newest tool for administrative automation: Windows PowerShell. Scripting guru Don Jones, co-author of ***Microsoft Windows PowerShell: TFM***, and a half-dozen other books on scripting and automation, introduces you to Windows PowerShell's interactive capabilities and its scripting language. You'll learn to use cmdlets, write basic scripts, and more. More importantly, you'll be able to perform real-world tasks like query Windows Management Instrumentation, work with Active Directory objects, manage computers' local security accounts, manage services, processes, and security, work with the registry, and much more. Bring a laptop with Windows PowerShell installed and be prepared to follow along as Don whizzes through the basics of this exciting new shell. Perfect if you're looking at Exchange Server 2007, which has its administrative functionality built upon Windows PowerShell!

9AM - 4PM • PRE-CONFERENCE WORKSHOP • OFFICE TRACK

OPR202: WINDOWS SHAREPOINT SERVICES DEMYSTIFIED

CA CALLAHAN

An IT professional's guide on how to install, set up, and administer WSS 3.0 with an overview of what it is and what it does. Includes topics such as what Windows Sharepoint Services are and how they differ from MOSS; what WSS does to the server under the hood; dos, don'ts, and best practices from an administrator's point of view; and what the heck a document library actually is. Learn what to consider when installing WSS; how to use preexisting libraries, lists, and other out-of-the-box goodies; how to create subsites (and why); how to manage users, rights, and configure settings that any administrator needs to know. Attendees will come away with a working knowledge of Windows Sharepoint Services and what to watch out for when deploying it in their business environment.

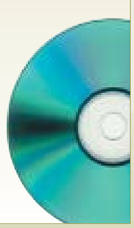
EVERY ATTENDEE RECEIVES

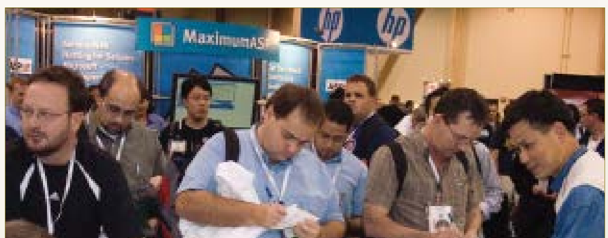
A one-year subscription to

Windows IT Pro

- Three Lunches
- Three Continental Breakfasts
- Reception
- Exchange Launch Party
- Proceedings Resource CD
- Conference T-Shirt and Bag

...and more





SPONSORSHIP/EXHIBIT INFORMATION

For sponsorship information, contact

Rod Dunlap

Tel: 480-917-3527

E-mail: rod@devconnections.com

SEE WEB SITE FOR MORE DETAILS.
www.WinConnections.com

WORKSHOPS

POST-CONFERENCE WORKSHOPS

9AM - 4PM • POST-CONFERENCE WORKSHOP • EXCHANGE TRACK

EPS301: EXCHANGE 2007 FOR EXCHANGE 2003 ADMINISTRATORS

JIM MCBEE

There has been a lot of hype and media attention surrounding Exchange 2007. The Exchange community has gotten their first look at Exchange 2007 in the summer of 2006. But what does the imminent release of Exchange 2007 mean to you as an Exchange 2003 administrator and your users?

64-bit hardware support, a revamped user interface through a new graphical user interface or Monad scripts, continuous replication, resource mailbox support, Edge services, improved mobile support, and unified messaging will all affect the way we manage our Exchange organizations and the services we provide to our user community. Topics in this workshop include:

- Determining a migration / upgrade path to Exchange 2007 from your current Exchange environment
- Implementing e-mail lifecycle management
- Implementing Outlook 2007 using the auto-discovery service
- Reviewing the new Exchange server roles
- Using new features for virus protection, spam reduction, and content filtering
- Using the new Exchange Management Console and Monad scriptlets
- Using local continuous replication to improve availability
- Implementing Exchange Edge services
- Reviewing new unified messaging features
- Taking advantage of resource mailboxes and the scheduling assistant

9AM - 4PM • POST-CONFERENCE WORKSHOP • WINDOWS TRACK

WPS301: REIMAGINING IT ADMINISTRATION: ROLE-BASED MANAGEMENT, PROVISIONING, AND ACCELERATED ADMINISTRATION

DAN HOLME

Find out why this workshop is consistently rated as a "best of breed" session, delivered as a capstone to your Windows Connections experience. From his work with thousands of IT professionals, from the CIOs of Fortune companies to front-line support professionals, Dan Holme has amassed a wealth of experience and expertise—solutions which enable you to deliver real-world best practices within the constraints of real-world budgets and technologies.

ROLE-BASED MANAGEMENT: You will discover how to implement role-based management, in which users are defined by their business roles and where resource access and configuration are instantly, accurately, and auditably applied. Empower your enterprise to enable a documented, auditable structure for resource security, asset management, and more.

PROVISIONING: You have the technology. Your business has processes. But too commonly they are not aligned. Learn how concepts of provisioning can enable you to support business processes through easy-to-implement solutions for scenarios including user management, new and replaced computers, and group membership tracking, to name a few.

ACCELERATED ADMINISTRATION: Learn the tricks that Dan has developed with enterprises large and small to facilitate administration and security. Dan will focus on creating highly customized and effective MMC consoles, scripts, intranet pages, and toolsets utilizing the native Windows administrative tools, support tools, and Resource Kit and free third-party utilities.

9AM - 4PM • POST-CONFERENCE WORKSHOP • WINDOWS TRACK

WPS302: CREATE A TEST ENVIRONMENT, VIRTUALLY AND INEXPENSIVELY (HANDS ON)

RHONDA LAYFIELD

Have you ever wanted a test environment, but didn't know where or how to start? Purchasing new hardware to sacrifice to a test network can be pretty costly, not to mention the amount of time it takes to build and maintain the test environment. While this task can seem overwhelming, it doesn't have to be. This post-conference workshop will give you hands-on experience in creating your very own test environment that mirrors your production environment with built-in disaster recovery! Now think about that for a second—regardless of the technology you require in your test lab, be it SQL, Exchange, Active Directory, or a development test environment, these step-by-step labs will work for all, and you get to perform them live.

Participants will be required to bring their own laptop (hardware requirements will be posted online), onto which they will install the free VMWare Server product, which will be used to create your own virtual test environment live, in class. You will also be able to take these step-by-step labs back to work with you and create your own virtual test environment, no muss no fuss, and no drain on your budget!!

9AM - 4PM • POST-CONFERENCE WORKSHOP • OFFICE TRACK

OPS201: MICROSOFT OFFICE SHAREPOINT SERVER 2007 (MOSS) WEB CONTENT MANAGEMENT

BOB MIXON

Microsoft Office SharePoint Server 2007 has included a very robust feature set called Web Content Management (WCM). In this full-day workshop you will learn how to plan for, design, and deliver a highly scalable Web Content Management Solution. You may have heard about Web Content Management, but what does it "really" do and what value does it add to my customers? This workshop will provide the details of what WCM is and why it is important. It will cover the high-level feature set that we will dive in to throughout the rest of our day. The most important step in any solution is to have a workable plan; without this, the risk of failure is very high. In this workshop we'll describe best practices for planning and documenting the design of your content management solution. In addition, you'll see a demonstration of how to create custom column types, content types, and associated page layouts.

Another exciting feature of Microsoft Office 2007 is workflow; without it, Web Content Management couldn't exist. This part of the workshop will describe and provide demonstrations of both simple and complex workflow scenarios that will be common in your workplace. You'll learn how these workflows can be attached to your custom content types and set for manual or automatic initiation. Once you have your Content Management solution in place, you will need to educate your content authors. With the new features found in Microsoft Office 2007, content authoring and publishing couldn't be easier. You'll see demonstrations of how content can be authored using Microsoft Word or the browser. In addition, I will show the role workflow plays during the authoring and publication process.

To wrap up the day, you'll learn various ways of aggregating content and displaying it on your site using the Content Query Web Part (CQWP). The Content Query Web Part provides a wealth of features, many of which are misunderstood. You'll see a demonstration of how to configure and customize this Web Part to get the results you are looking for.

SESSIONS AND SPEAKERS ARE SUBJECT TO CHANGE.
SEE WEB SITE FOR UPDATES AND ADDITIONAL SESSIONS.

EVENT INFORMATION

HOTEL INFORMATION

HOTEL ACCOMMODATIONS

The Hyatt Regency Grand Cypress Resort, One Grand Cypress Blvd., Orlando, FL is the conference site and host hotel. SPACE IS LIMITED so reserve your room early by calling the conference hotline at 800-505-1201.

AIRLINE

Please call Pericas Travel at 203-562-6668 for airline reservations.

CAR RENTAL

Hertz is offering auto rental discounts to attendees. Call the Hertz Meeting Desk at 800-654-2240 for reservations and refer to code CV# 010R0031 to receive your attendee discount.

AIRPORT SHUTTLE

Mears Transportation is the designated ground carrier at Orlando International Airport. The shuttle may be picked up at Level 1 of the airport. The shuttle is available 24 hours a day. The rates to the Hyatt Regency Grand Cypress hotel are as follows: One-way is $18.00 and $30.00 round-trip. You may call Mears directly at 407-843-2404 for more information or go to their Web site www.mearstransportation.com. Prices are subject to change.

ATTIRE

The recommended dress for the conference is casual and comfortable. Please bring along a sweater or jacket, as the ballrooms can get cool with the hotel's air conditioning.

ORLANDO, FLORIDA

EXTEND YOUR STAY

Come early or stay late. Bring the family! You are in the land of fantasy for children of all ages. Walt Disney World - Magic Kingdom® Park, Disney MGM Studios®, Epcot® and Disney's Animal Kingdom® Theme Park. In addition, explore Kennedy Space Center, Sea World, and Universal Studios Theme Park, or take a short drive to beautiful white sand Atlantic beaches.

TAX DEDUCTION

Your attendance to a DevConnections conference may be tax deductible. Visit www.irs.ustreas.gov. Look for topic 513 - Educational Expenses. You may be able to deduct the conference fee if you undertake to (1) maintain or improve skills required in your present job; (2) fulfill an employment condition mandated by your employer to keep your salary, status, or job.

SPONSORSHIP/EXHIBIT INFORMATION

For sponsorship information, contact:
Rod Dunlap
phone: 480-917-3527
e-mail: rod@devconnections.com
See web site for more details. www.WinConnections.com

GROUP DISCOUNT

Register individuals from one company at the same time and receive a group discount.

Call 800-505-1201 to take advantage of group discount pricing.

1-3 registrants	$1,395 per person
Additional registrants after the 3rd (4th, 5th, 6th...)	$1,195 per person ($200 off each)

NOTES & POLICIES: The Conference Producers reserve the right to cancel the conference by refunding the registration fee. Producers can substitute speakers and topics and cancel sessions without notice or obligation. Updates will be posted on our Web site at www.WinConnections.com. Tape recording, photography is not allowed at any session. Conference producers will be taking candid pictures of events and reserve the right to reproduce. By attending this conference you agree to this policy. You may transfer this registration to a colleague. Please inform us if you have any special needs or dietary restrictions when you register. The conference registration includes a one-year print subscription to *Windows IT Pro*. Current subscribers will have an additional one year added to their subscription. Subscriptions outside of the United States and Canada will be digital. $25 of the funds will be allocated toward a subscription to *Windows IT Pro* ($49.95 value). **REGISTRATION & CANCELLATION POLICY:** Registrations are not confirmed until payment is received. Cancellations before March 1, 2007 must be received in writing and will be refunded minus a $100 processing fee. After March 1, 2007 cancellations and no shows are liable for full registration, it can be transferred to the next Connections Conference within 12 months or to another person. Active Directory, Microsoft, MSDN, Outlook, Windows NT, Windows Server, Windows Vista, and Windows are either trademarks or registered trademarks of Microsoft Corporation. All other trademarks are property of their owners.

CONFERENCE REGISTRATION • APRIL 1-4, 2007

FULL CONFERENCE REGISTRATION INCLUDES KEYNOTE ON APRIL 1, 6:30PM, THROUGH CLOSING SESSION APRIL 4, 4:30PM

NAME PRIORITY CODE

COMPANY TITLE

STREET ADDRESS (REQUIRED TO SHIP MATERIALS)

CITY, STATE, POSTAL CODE COUNTRY

TELEPHONE FAX E-MAIL ADDRESS (IMPORTANT)

ONLINE
www.WinConnections.com

E-MAIL
info@devconnections.com

PHONE
(800) 505-1201, (203) 268-3204

FAX
(203) 261-3884

MAIL
Microsoft Exchange Connections 2007
Windows Connections 2007
Office Connections 2007
c/o Tech Conferences, Inc.
731 Main Street, Suite C-3
Monroe, CT 06468

❏ **Microsoft Exchange Connections** ....on or before February 15 ....$1295.00 ________
....after February 15 ....$1395.00 ________

❏ **Windows Connections** ....on or before February 15 ....$1295.00 ________
....after February 15 ....$1395.00 ________

❏ **Office Connections** ....on or before February 15 ....$1295.00 ________
....after February 15 ....$1395.00 ________

SPECIAL BONUS HANDS-ON COURSES

If you are registering for the conference and would like to take one or more of the following hands-on courses, please make your selection here. Space is limited. If the class is full, you will be notified when your registration is received.

- ❏ MONDAY, APRIL 2, 2007 — Troubleshooting Disaster Recovery with Exchange Server 2003 (full day)
- ❏ TUESDAY, APRIL 3, 2007 — Troubleshooting Message Flow in Exchange Server 2003 (full day)
- ❏ WEDNESDAY, APRIL 4, 2007 — Troubleshooting Performance in Exchange Server 2003 (full day)

- ❏ MONDAY, APRIL 2, 2007 — VBScript Master Course (bring your own laptop)
- ❏ TUESDAY, APRIL 3, 2007 — PowerShell Master Course (bring your own laptop)

PRE-CONFERENCE WORKSHOPS SUNDAY, APRIL 1, 2007 LUNCH IS INCLUDED WITH FULL DAY WORKSHOPS.

- ❏ 9:00AM - 4:00PM — Microsoft Exchange Server 2007 Hands-on Labs O'DOWD ....$399 ________
- ❏ 9:00AM - 4:00PM — Reimagining the Image: Deploying, Repairing, Replacing, and Updating Windows XP and Windows Vista Client HOLME ....$399 ________
- ❏ 9:00AM - 12:00PM — VBScript Basic Training JONES ....$199 ________
- ❏ 1:00PM - 4:00PM — Windows PowerShell Basic Training (bring your own laptop) JONES ....$199 ________
- ❏ 9:00AM - 4:00PM — Windows SharePoint Services Demystified CALLAHAN ....$399 ________

POST-CONFERENCE WORKSHOPS THURSDAY, APRIL 5, 2007 LUNCH IS INCLUDED WITH FULL DAY WORKSHOPS.

- ❏ 9:00AM - 4:00PM — Exchange 2007 for Exchange 2003 Administrators MCBEE ....$399 ________
- ❏ 9:00AM - 4:00PM — Reimagining IT Administration: Role-Based Management, Provisioning, and Accelerated Administration HOLME ....$399 ________
- ❏ 9:00AM - 4:00PM — Create a Test Environment, Virtually and Inexpensively (Hands-on - bring your own laptop) LAYFIELD ....$399 ________
- ❏ 9:00AM - 4:00PM — Microsoft Office SharePoint Server 2007 (MOSS) Web Content Management MIXON ....$399 ________

CONFERENCE MATERIALS

Full conference registration includes materials for the one conference for which you register. You may purchase materials for the other concurrently run events.

- ❏ Microsoft Exchange Connections Proceedings Book and Resource CD ....$99 ________
- ❏ Windows Connections Proceedings Book and Resource CD ....$99 ________
- ❏ Office Connections Proceedings Book and Resource CD ....$99 ________

PAYMENT TOTAL

*IMPORTANT: You must reference Microsoft Exchange Connections, Windows Connections, or Office Connections on your check.

❏ CHECK (payable to Tech Conferences) All payments must be in US Currency. Checks must be drawn on a US bank.

❏ VISA ❏ MASTERCARD ❏ AMEX

CREDIT CARD NO. EXPIRATION DATE

Cardholder's Signature Cardholder's Name (print)

MICROSOFT
EXCHANGE
Connections
2007

WINDOWS
Connections
2007

Office
Connections
2007

Microsoft, *Windows IT Pro*, *TechNet Magazine* and Tech Conferences come together to bring you the premier event for IT Professionals.

April 1-4, 2007

Orlando, Florida
Hyatt Regency Grand Cypress Resort

Microsoft® Windows IT Pro TechNet Magazine Tech Conferences Inc. PENTON MEDIA

Register Today! • WinConnections.com • 800-505-1201 • 203-268-3204

WinConnections 2007
c/o Tech Conferences, Inc.
731 Main Street, Suite C-3
Monroe, CT 06468

Mailroom: If addressee is no longer here,
please route to MIS Manager or Training Director

library, select one or more slides, then click *Copy Slide to Presentation.* SharePoint launches PowerPoint and creates a presentation with the selected slides.

Can you imagine how happy your communications team will be to create "standard" slides that can be reused, instead of reinvented, and can be managed (updated and deleted) centrally? This might be the best thing to ever happen to PowerPoint. My clients' dreams of consistent communications might actually begin to come true.

Experience SharePoint

Many of my clients are IT organizations that need to know what "low-hanging fruit" can be picked with SharePoint Server. I hope the experiences I've led you through so far will give you something to show your management or other stakeholders in your organization and will give you the confidence and interest to approach SharePoint Server yourself and get acclimated to its capabilities.

InstantDoc ID 94652

Dan Holme

(danh@intelliem.com) is director of consulting at Intelliem, which delivers solutions-focused training and consulting services supporting enterprise SharePoint, Office, Windows, and Active Directory implementations.

Figure 5:
Document Library Actions

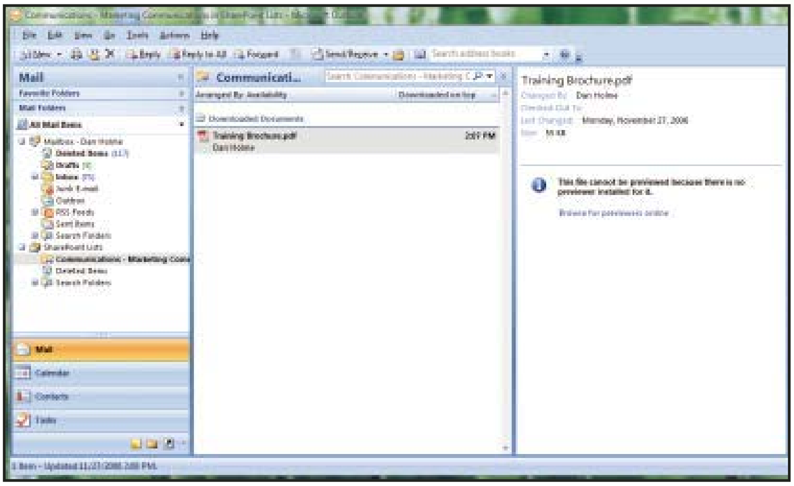


Figure 6:
Document Library in Outlook

Something New at the Office

Introducing the new Office servers

by Dan Holme

Microsoft officially launched a staggering number of new products, including Windows Vista and the Microsoft Office System 2007, on November 30, 2006. Several of these products were upgrades of previous releases; however, a significant number of new Office servers were included in the Office 2007 release.

Cynics might suggest that the new Office server products are Microsoft's way of squeezing more revenue out of the Office product line, which is already installed on nearly every information worker's computer. Revenue certainly would have been a consideration for Microsoft. However, many businesses need the solutions that the new Office servers offer to accommodate the changes in the way today's information workers do business. Businesses and their partners, customers, and end users are now demanding collaboration solutions, automated business processes, auditing and compliance, and access to information anytime and anywhere.

In the current Office client suite, there are many applications—and not all of them are appropriate for every business, scenario, or user. For example, many users never have to use Microsoft Access or Microsoft Office Publisher, although few can do their jobs without using Microsoft Word or Microsoft Excel. The same will hold true for the new Office server applications. Each server product serves a specific need, and although some tools (such as Microsoft Office SharePoint Server) will become ubiquitous, others (such as Microsoft Project Server) will probably be limited to a niche in the market.

Most companies will find that one or more of these server products can deliver real business value to their organizations. I've found that effective collaboration can give a company a significant competitive advantage.

The problem has been that, until now, collaboration application solutions have typically been expensive both in terms of capital

outlay for the software and training for end users. These applications are also often difficult to integrate into existing business processes. In most cases, the early adopters of collaboration solutions found there was no return on their investments because they had to overcome significant obstacles to successfully implement the tools or the end users didn't use the tools because the learning curve was so high. If implemented into your environment correctly, the new Office servers can deliver the crucial balance of power and flexibility (for you) and familiarity (for your users) that can lead to a successful collaboration solution. To help you with the implementation, let's examine each of the new Office server products—Forms Server 2007, Groove Server 2007, Project Server 2007, and SharePoint Server 2007—so that you can understand their purpose and better evaluate their potential role in your business collaboration strategy.

Forms Server 2007

What business doesn't have forms? Many businesses use paper forms whose appearance and processing haven't changed much in years. Forms Server 2007 is a standalone server that delivers and manages digital forms that replace paper forms and legacy online forms (such as fill-in PDF files). You can access the forms through Microsoft Office InfoPath 2007 or a Web browser for data collection, distribution, and integration with processes using business rules.

Authorized users create forms using InfoPath 2007. You can use controls (such as text boxes and drop-down lists) that Forms Server 2007 makes available. You can preconfigure the behavior of each control. For example, you can preconfigure mouse-over tips, prepopulated default values, and data validation. Additional behaviors connect the form and its controls with back-end systems, such as SharePoint Server 2007. You can then place the forms into a SharePoint Server 2007 or Microsoft BizTalk Server 2006 workflow.

All of the heavy-lifting application code and primary business logic rules are configured and executed on the server, which means a form's creator or user can build what he or she needs while developers control the precise and complete integration of the form, its data business processes, and its workflows. As forms are updated, new versions can be deployed side-by-side with reusable controls and business logic.

You can use InfoPath 2007 (or other third-party applications) as a standalone application to create electronic forms, but if multiple forms need to work together within a process or if external clients need access to those forms through a browser, you'll need IT to build a solution to support it. However, Forms Server 2007 can easily move forms online, create workflows, and centralize data management. Keep in mind that you can host forms on SharePoint Server 2007, so take advantage of this ability if you're already using it. Forms Server 2007 is a standalone product and cheaper than SharePoint Server 2007, but it's for environments that need only the forms capability. I've found that the most difficult part of implementing Forms Server 2007 is combining all the scattered paper and online forms into a defined business process. You'll need to invest time to analyze your business and implement a structure of forms, business logic, and workflows.

Groove Server 2007

If you've yet to select a set of tools to use to provide a collaborative workspace (or even if you already have), you should take a look at Groove Server 2007. Groove 2007 workspaces provide tools for file sharing, discussions, meetings, specialized calendars, and presence awareness (i.e., knowing who is online). Business forms are available through InfoPath 2007, with phone calls and IM available when Groove Server 2007 is integrated with Microsoft Office Communicator. Groove Server 2007 also lets you make SharePoint Server 2007 sites available offline.

From a user's perspective, a Groove 2007 workspace is simple to create and maintain: With only a couple of clicks, you can create a Groove 2007 workspace on a local computer. Users can then share that workspace with other users (think workgroup), which is sufficient for small- to medium-sized workspaces.

When the connection to external data sources and complexity of the workspace environment (e.g., size of the workspace, dispersion of clients) overload the decentralized workgroup environment, workspaces can be managed on the Groove server. This architecture lets you maintain data versions and update postings centrally, but lets users store their working copies locally. That means when users travel or work offsite, they don't have to be connected to Groove Server 2007 to work on documents, post discussion questions and comments, or add items to the workspace. The next time that users connect to Groove Server 2007, the updates on their computers are automatically synchronized to Groove Server 2007, and all other users' workspaces are updated on their local computers.

On the back end, there are several components that need to be configured properly to keep server-managed workspaces up-to-date while not bringing down the network (just kidding, but there is overhead to plan for). The Manager (for defining workspaces), Relay (for controlling site-type traffic), and Data Bridge (for connecting to Microsoft SQL Server or other databases) server components are all part of the infrastructure that supports workspaces. Collaboration tools have huge front-end productivity gains, so the resources that businesses invest usually have a significant ROI. The resources needed for Groove Server 2007 will also be compensated, to some degree, by users not having to email large attachments back and forth multiple times. For example, a Microsoft Office PowerPoint presentation can be edited locally and synchronized by Groove Server 2007, so that there aren't multiple versions of the presentation in multiple users' mailboxes on the mail server.

Groove was a successful application, even before Microsoft acquired Groove Networks in April 2005. There are clearly scenarios in which decentralized collaboration plays an important role. Certainly, some collaboration scenarios outside your network might be better supported by Groove Server 2007 than by a SharePoint Server 2007 extranet. Groove Server 2007's ability to make certain that SharePoint Server 2007 data is available offline might also be attractive to some users. At the lower levels of implementation, you can deploy Groove Server 2007 for users similarly to how you deploy Office and other user-productivity applications today.

When the workgroup model becomes overwhelmed or insufficient, you should develop a Groove Server 2007 topology. This article isn't the place for a detailed discussion, but a Groove 2007 implementation is similar to any other messaging implementation with load, relay, and storage considerations that need to be planned for. Microsoft Exchange Server 2007 provides even more integration possibilities. Developers will be glad to learn that the Groove 2007 workspace integrates with InfoPath forms and SharePoint Server 2007 document libraries to keep data consistent across high-level business processes. Although InfoPath forms and SharePoint Server 2007 document libraries are for users, administrators can use them for planning and defining those business processes.

Most businesses likely won't consider using Groove Server 2007 until after SharePoint Server 2007 has been rolled out. Even then, businesses will be wise to seek guidance from Microsoft or Groove-savvy IT consultants to properly implement Groove Server 2007 so that it meets their business needs.

Project Server 2007

Project Server 2007 extends the power of previous versions of Project Server and embraces more of the toolset that's used across the enterprise on the ground level, particularly Excel and Microsoft Office Outlook. For example, you can use Outlook to maintain tasks (such as progress, completion, and change schedule) and handle reports in Excel or Microsoft Office Visio that are dynamically tied back to the data on the Project Server. If a browser is more to users' liking, Microsoft Office Project Web Access and Project Workspace let users collaborate over the Web. It's always positive when users can facilitate high-level processes without a learning curve.

At higher levels of project management, the Cube Building Service enables you to use portfolio analyzer cubes for sophisticated analysis and reporting. Resource plans can show high-level resource allocation for categories of proposed projects without digging into unnecessary details. Timesheets now support fiscal periods and cost codes, and other financial fields that let you report hours separately from the progress made on tasks. You can also define deliverables, and those deliverables can cross projects. These additional functions are likely to increase Project Server 2007's attractiveness as a solution within part of the original collaboration solutions.

Project Server 2007 offers welcome improvements for developers. Now fully implemented on the Microsoft .NET Framework, it's not as difficult to reach Project Server 2007 from the outside, as the API now exposes all the functionality and data that client applications might need. Project Server 2007 also supports the Windows Workflow Foundation (WF), which allows for the integration of business processes defined and implemented within the context of other Office servers. From the performance side, the scheduling engine has been moved to the server, meaning that custom front ends no longer require the full executable (winproj.exe) on each machine.

With Project Server 2007, users will be able to manage their projects more easily within the context of familiar tools, project managers will get more features and better reporting capabilities, and developers will get easier access to data that used to be much harder to reach. If your organization already uses Microsoft Project, you can certainly expect Project Server 2007 to be part of your collaboration solutions, especially as demand for good reporting increases. (Note: Not every user needs to be a project manager to use Project Server 2007.)

SharePoint Server 2007

SharePoint Server 2007 is the "Mother Hen" that brings people and data together within defined contexts. What started several years ago as a document library and fledging communication tool has developed into a robust information portal. Although chances are that you've worked with SharePoint at some point, there are many new and improved features. SharePoint Server 2007 serves the following six business scenarios:

Portal. SharePoint Server 2007 supports designing, deploying, and managing enterprise intranet portals, corporate Internet presence Web sites, and divisional portal sites. The portal components also make it easy to connect to people who have the right skills, knowledge, and project experience.

Users get a personalized experience because of user profiles, audience targeting, presence awareness, and audience-appropriate views (such as My Manager and My Assistant). An LDAP-pluggable provider (in addition to the Active Directory—AD—provider) lets you securely access categorical information based on the various directory services that might be involved.

Enterprise Search. SharePoint Server 2007 lets you access data repositories across your enterprise and provide search results that are relevant to your enterprise and that respect security (i.e., only show results that you have permission to read). Think of Enterprise Search as an inhouse Google. (I can hear the shudders of folks at Microsoft as I compare Enterprise Search to Google, but they'll get over it.)

Content management, including documents, records, and Web content. What used to be a simple platform for document collaboration is now a full-featured solution for managing business documents and content. Going far beyond a simple repository for documents, SharePoint Server 2007's libraries are configurable for submission, review, approval, and signature processes surrounding any document, regardless of whether the document was created in an Office application or through a Web editor interface. These managed document libraries are controlled by templates that provide the business logic for controlling workflows, translating documents into any of the 28 supported languages, and rolling up documents into comprehensive reports.

Business processes. The client/server platform (InfoPath Form Services) enables you to create, deploy, and maintain centrally managed forms. Related data is XML-based, is Web accessible, and can be integrated into back-end business processes.

SharePoint Server 2007 provides access to defined data within a business process through single sign-on (SSO), which permits a user to enter only one username and password to use a variety of back-end applications in addition to those controlled directly by SharePoint Server 2007. Once authenticated, the business user has access to all configured forms within the workflow.

Forms are based on XML schemas that you define to control the structure of the data captured by the form, whether the form is created directly in InfoPath 2007 or imported from an existing Word or Excel document. A completed form is an XML file that complies with that structure, making it highly actionable. For example, a loan application form might include a main view for an applicant to fill in data using a browser and another view visible to only the loan officer, who reviews and approves the application.

Business intelligence. SharePoint Server 2007 enables you to develop Web-based business intelligence (BI) dashboards that can incorporate rich, data-bound Key Performance Indicators (KPIs), Web Parts, and published spreadsheets. Analysis is key for BI, and the familiar tool for business users is Excel, so it's not surprising that SharePoint Server 2007 heavily leverages it. SharePoint Server 2007 can refresh external data, recalculate workbooks, and render them with a high-fidelity, Web-based UI in an Excel Web Services Web Part. Based on publishing parameters, SharePoint Server 2007 can render a complete Excel 2007 workbook, select worksheets, or select a region within a worksheet.

Developers can use Excel Web Services to calculate a complex model built in Excel 2007 and display the results to a user working on a Web-based UI or custom desktop application. SharePoint Server 2007 includes out-of-the-box Web sites, that are hosted by the new Report Center, which has been optimized for report access and management. Integration and aggregation with SQL Server Reporting Services (SSRS) into a SharePoint Server 2007 Business Data Catalog extends reporting capabilities even further, making appropriate data readily available to the business user.

SharePoint Server 2007 gives you the ability to efficiently manage data for business processes, provide collaboration at numerous levels within team workflows, and secure access for all business users. Solid planning, a logical implementation strategy, and timely user training should result in a healthy ROI. But with six business scenarios covered by SharePoint Server 2007 alone, it's easy to get overwhelmed. Pick one or two scenarios that are most important to your business to focus on, but don't lose sight of SharePoint Server 2007's other capabilities because chances are good that as users experience SharePoint Server 2007, they'll start requesting solutions covered in the other scenarios.

SharePoint Server 2007 has the potential to unlock enormous productivity potential when aligned with business processes and strategies. Although the financial markets have been focused on how many copies of Windows Vista and Office 2007 Microsoft will sell, it's really SharePoint Server 2007 that's the stealth force.

What the New Office Servers Mean for You

The Office 2007 servers focus on collaboration, and I think IT can (and should) expect this upgrade cycle of Office to go beyond a simple discussion of user-level features. Many businesses are at the tipping point for collaboration—it isn't just a good idea to have managed collaboration, it's necessary, and collaboration solutions require a great deal of planning beyond a normal upgrade of the desktop product. Your Office servers planning and implementation efforts will be similar to when you planned for directory services (i.e., going from the workgroup to the domain mentality).

The days of simply providing users with applications are over. The unique workflows in today's businesses involve data and people, and office tools need to be configured to meet the needs of those workflows. With an Office 2007 environment, you can make data available to the correct people, properly secure that data, and provide users with the tools they need to achieve their business goals. Early adopters of the Office 2007 collaboration tools are proving that the tools work well and that productivity gains are huge when you invest the time and resources needed for up-front planning and a good user-training program. SharePoint Server 2007 is necessary, and the supporting tools fill specific roles—you can expect high demand from both users and business owners for increased collaboration.

InstantDoc ID 94492

Dan Holme
(danh@intelliem.com) is the director of training at Intelliem, which delivers solutions-focused training and consulting services that support Windows and Active Directory implementations at enterprises.

Getting to Know Office 2007

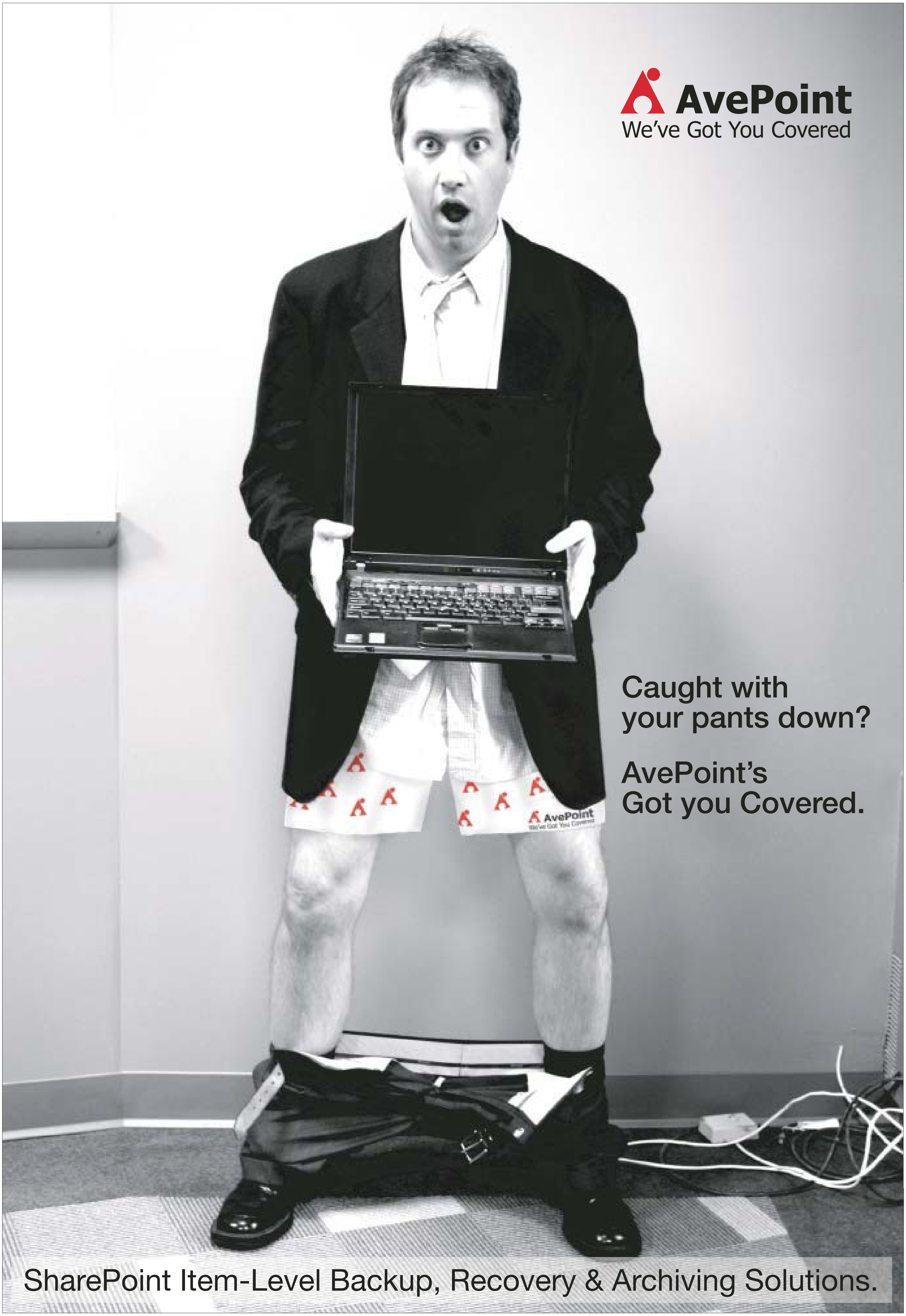
Answers to your questions about the new Microsoft Office 2007 System

by Dan Holme

Q: Will Microsoft Office 2007 System updates be easier to deploy to users?

A: Yes. In previous Office versions, you kept local installations current by updating the source files in the administrative installation point and triggering a reinstallation of Office on each user's computer. Or you configured Office 2000 Setup to chain software updates with new installations of Office. Keeping all installations synchronized was difficult.

Now, you create a network installation point that you never have to update, so that client computers never become out of sync with the installation source. Keeping new installations current is as simple as copying updates to a folder on the network installation point. There's no need to configure complex, chained deployments or modify the original installation files. New installations will chain the updates in sequence, and you can specify different locations for updates by using a config.xml file. (For more information about deployment mechanisms, see the Microsoft article "Deploy the 2007 Office system with limited network capacity" at http://technet2.microsoft.com/office/en-us/library/1f721083-6d58-4a53-


AvePoint
We've Got You Covered
Caught with
your pants down?
AvePoint's
Got you Covered.
SharePoint Item-Level Backup, Recovery & Archiving Solutions.

94c1-1bbfc36a249b1033.mspx.)

For organizations that subscribe to Windows Server Update Services (WSUS), I highly recommend that you install Office 2007 with cached installation files and distribute updates by using WSUS.

Q: What can I really expect from Office 2007?

A: Your users are definitely in for an adjustment as they experience the new UI. Be proactive in training and preparing them. In my experience with clients, organizations that have introduced users to the new UI, with as little as a 30-minute introduction, have found the transition to be significantly smoother than those that haven't prepared end users. Microsoft provides several Office 2007 resources (e.g., training and command-reference guides) at http://office.microsoft.com, which you can incorporate into your end-user training.

Once the adjustment is made, the experience of Office 2007 early adopters confirms that the new UI enables users to be significantly more productive. In addition, the new file formats and deployment processes are easier for IT administrators to manage. Most importantly, the power of Office 2007, which includes Windows SharePoint Services and support for technologies such as information rights management (IRM), means that collaboration, knowledge management, business intelligence, and security will add real business value. This isn't just Microsoft hype; I've seen it firsthand. And as Office 2007 rolls onto desktops, we'll all begin to gather real-world experience with the good, the bad, and the ugly in the newest overhauled Office version.

Q: Has the number of rows and columns supported by Microsoft Office Excel 2007 changed?

A: The long-standing limitation of 256 columns (A to ZZ) and 16,384 rows has been expanded to include worksheets up to 16,384 columns (A to ZZZ) and 1,048,576 rows.

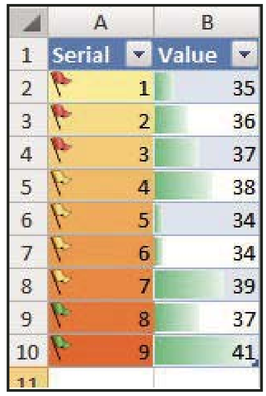
Q: Will my computer have enough horsepower to run Office 2007?

A: Most likely, yes, if you're using a computer purchased within the last year or two. However, Microsoft has changed how it states an application's hardware prerequisites, and Microsoft's numbers sometimes assume that you're running nothing but Office 2007. Check out Table 1 to see Microsoft's stated system requirements for Office 2007 versus what I think are probably more realistic requirement guidelines.

Q: Excel 2007's conditional formatting has additional settings; what are they?

A: Figure 1 shows examples of the three new settings for Conditional Formatting: Color Scales, Icon Sets, and Data Bars. Color Scales color the background of a group of cells with different colors according to the values of the various cells. For example, in the Serial column in Figure 1, the color of the successive cells gradually changes from yellow to red as the cell values increase. Icon Sets precede the text in a cell with an icon that represents some aspect of the cell's value with respect to other values in a group of cells. In Figure 1, cells are marked as belonging to a specific group by a colored flag that precedes the integer in the Serial field. Data Bars show a gradient bar in a cell's background and can display information that might not be explicitly stated (i.e., with a numerical value) in the field.

Q: I'm a little confused about differentiating themes, templates, and Quick Styles. Can you clarify what each of these features does, or at least point me in the right direction?



	A	B
1	Serial	Value
2	1	35
3	2	36
4	3	37
5	4	38
6	5	34
7	6	34
8	7	39
9	8	37
10	9	41

Figure 1: ***Sample spreadsheet showing new conditional-formatting settings in Excel 2007***

A: Your confusion is understandable, especially about themes, which are an entirely new feature, although older versions of Office had a (different) feature called "themes." An Office 2007 theme is a new, standalone file type (.thmx) that defines colors, fonts, and effects to create a distinctive, visually cohesive look for all Office 2007 documents. Default themes include Office, Urban, and Opulent. You can find them in the themes gallery in each application: on the Design tab in Microsoft Office PowerPoint 2007 and on the Page Layout tab in Microsoft Office Word 2007, Microsoft Office Outlook 2007 email messages, and Excel 2007.

Every Office 2007 document has a theme associated with it. Themes are available across Excel 2007, Word 2007, PowerPoint 2007, and Outlook 2007. Therefore, your communications or design personnel should spend some time, right away, creating themes that reflect your corporate identity.

In Office 2007, a template is truly a starter document. For example, PowerPoint 2007 design templates have been replaced by themes, and each theme defines slide layout, colors, and other slide-design features. PowerPoint 2007, on the other hand, now contains only starter slides and boilerplate content.

Table 1: Office 2007 Requirements: Microsoft's Versus Dan's

Stated Requirements	More Realistic
500MHz or faster processor	2GHz or faster if you run multiple applications, and who doesn't keep Outlook 2007 open all the time?
256MB RAM or more	1GB or more if you want all the Instant Search options, such as OneNote 2007's audio searching and Word 2007's contextual spelling, to work. 512MB is the minimum workable space for basic features.
1.5GB or more hard disk space	That's about right if you leave the setup files on the hard disk.
1024 × 768 display	That's about right. PowerPoint 2007 has support for wide-screen displays, too. (Now, about that new wide-screen projector....)

Got questions about Microsoft Office?

Send them to Dan Holme at danh@intelliem.com. And for more Office tips and insights, visit http://www.MyMSOfficePro.com, an upcoming new community for IT professionals, developers, and end users interested in Microsoft Office topics.

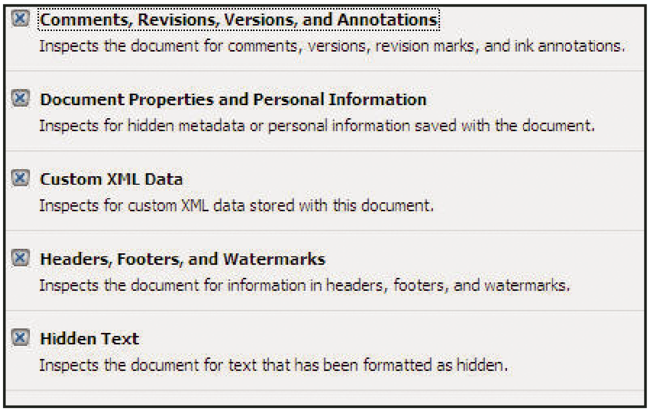


Figure 2:
Enabling Document Inspector features

PowerPoint 2007 shape styles, Excel 2007 cell styles, Word 2007 styles, and Quick Styles are affected by the colors, fonts, and effects of the theme that's in use. For example, in Word 2007 a template's Quick Style might define the Heading 1 style as a certain size and with a particular indentation. However, the theme would determine the actual font. A theme might be one of the built-in themes or one created with your corporate fonts and colors.

The theme defines, among other things, the font used for headings and that used for body text. The heading font defined in the theme would be sized and indented based on the Heading 1 style definition. What's great is that you could switch between a casual Quick Style and a more formal Quick Style, which would alter font sizes, indentation, and other aspects of text styles, but the colors and fonts would still comply with your corporate standards. Additionally, you could create Excel 2007 worksheets, PowerPoint 2007 presentations, and even email messages all using the same theme! Note, however, that one caveat of the theme function is that Microsoft Office 2003 documents and documents saved in Office 2003 formats will continue to behave as they always have. If, for example, you save a 2007 document as a 2003 document, any custom theme information defined in that file will be lost.

Q: I read about, but can't find, the Document Inspector on any of the Ribbon commands. What does the Document Inspector do, and how can I use it?

A: The Document Inspector is a prepublishing feature and doesn't live on the Ribbon (so to speak). Document inspection is available in Word, Excel and PowerPoint 2007. To find the Document Inspector, follow these steps:

1. Click the Office button.
2. Choose Prepare.
3. Click Inspect Document.

The inspection process removes categorical personal data and any tracked-changes identification. The list in Figure 2 shows the Document Inspector features you can enable.

InstantDoc ID 94533

—Dan Holme

The Sky Is Falling

3 rules for managing a crisis

A few years ago, I was a speaker at a series of *Windows IT Pro* events about security. Mark Minasi was also a speaker and would claim that he knew the secret to being a security guru and was going to teach it to everyone in the audience. He would then ask the audience to stand up and repeat after him: "The … sky … is … falling." Funny. Of course, this joke does beg the question: What would you do as an IT manager if someone came to you—from your company's security team or elsewhere—and made this exclamation? In any crisis situation, perceived or real, the speed at which decisions are made and the pressure felt by the individuals making them can lead to mistakes. Here are three rules to follow when you're managing a crisis situation. With a little practice, you can make dealing with emergencies as routine as a trip to the grocery store.

Rule 1: Stay Calm

Stay calm, both inwardly and outwardly. Becoming agitated will negatively affect your decision making and could spread panic. The people around you will likely become excited, emotional, and fearful—particularly if they feel they might be at fault. Be sure to smile, thank people for their help, and keep a positive yet realistic attitude. Your staff will be looking to you to be a leader and need to believe that the crisis will be averted or resolved, so it's your job to remain in control.

Rule 2: Drive for Certainty

Part of what drives panic in a crisis is the unknown. To remove this pressure, drive for certainty from the outset. As people bring you information, calmly ask where it came from, how it can be verified, and who is responsible for reporting any change in the information to you. Doing so will help you separate facts from fancy. If the alleged disaster really is a disaster, you need to be able to make decisions based on verifiable facts as often as possible, or else risk spending time on the wrong problems or even amplifying panic. Initially, you'll want to establish the following:

- What is at risk?—How effectively you respond to the situation will largely be determined by what's at risk. Consider the following scenarios: Customers can't use their line of business (LOB) software; a tornado is approaching the building; a VP can't log on to his or her computer. Each of these situations might constitute an emergency that you have to deal with, but each is unique because of what's at risk—the business continuity of a division, human safety, or the business continuity of a user (albeit an influential one).
- Who was the first observer?—Determining who the first person was to observe the situation helps you establish a timeline in which to place other observations, and also provides an excellent place to start investigating the facts.
- What is the scope of the symptoms?—Determine exactly what's affected and when it was affected. Plot the logical and physical locations on a diagram and log the time on the master timeline. Plotting these things will help you look for the cause of the problem and for what might be affected next.
- What would a successful outcome entail?—Determine early on the successful resolution to the crisis so that you can focus your efforts on success rather than on chasing dead-end leads or getting lost in details. For example, if an LOB application isn't available to a call center, the immediate goal is to restore the service, whether you find the source of the problem or not. You might solve the problem by initiating a business-continuity plan to move users to a different LOB server or by switching to a manual backup process.
- Who else needs to be involved?—From the previously mentioned items, determine who you need to work with to successfully reach the goal that you've identified and what information and assistance you'll need and when you'll need it.

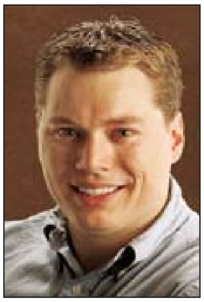
Rule 3: Communicate Clearly and Consistently

Few things amplify a crisis like confusion. On a whiteboard or wall, use Post-it Notes to create four columns, each with a heading describing the trust level of its information: *Verified fact, Believed to be true, Rumor, Untrue*. Place each piece of information that's reported to you into the appropriate column. Regularly report the overall status of the situation, the information gathered according to rule 2, and any other relevant information (along with the corresponding trust level), to the appropriate stakeholders. Over time, try to move all the information that's reported to you into either the *Verified fact* or *Untrue* column.

Controlling Crisis Situations

Following these three fundamental rules will make responding to any incident less taxing for you and everyone around you. These rules will help you control the emotions, uncertainty, and confusion that are all endemic to a crisis situation. In reality, situations in which the sky is falling occur rarely, but practicing this column's advice—even in the course of routine operations—will prepare you for the worst.

InstantDoc ID 94440

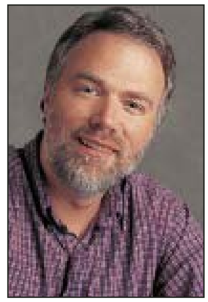


Ben Smith

Ben Smith (bensmi@microsoft.com) is a security strategist at Microsoft, where he researches methods to help organizations achieve better security through improved management and measurement techniques. He is coauthor of *Assessing Network Security* (Microsoft Press).

Unleashing SC on Service Configuration

One more look at this tool reveals its true power



Mark Minasi
(http://www.minasi.com/gethelp) is a senior contributing editor for *Windows IT Pro*, an MCSE, and the author of *Mastering Windows Server 2003* (Sybex). He writes and speaks around the world about Windows networking.

Ready to finish our look at SC (sc.exe), the command-line tool that offers wide-reaching control over services? In previous columns, I've demonstrated how SC lets you start and stop services, create new ones, delete existing ones, and control dependencies between services. But that's not all you can do with services. For example, I often find myself changing a service's startup status—whether it starts automatically or manually, whether it's disabled, and so on. You can control startup status, and much more, by using the SC Config command.

How It Works

The SC Config command largely mirrors the SC Create command, which I've covered before. Its overall syntax looks like

```
sc config <servicekeyname> <option= value>
  <option= value>
```

Here's an example that will illustrate this command's usefulness: Ever since Windows Server 2003 Service Pack 1 (SP1) and Windows XP SP2 disabled the Messenger service, I've gotten pretty regular email from people who say they need it. (Some folks *really* like the Net Send command.) To configure the Messenger service to automatically start every time you boot your computer, you could type

```
sc config messenger option= auto
```

(Recall that SC has the syntactic quirk of requiring a space between the equals sign and the option's value.) The other possible values are *boot, system, demand* (i.e., manual), and *disabled*.

By the way, Windows Vista systems have yet another possible value—*delayed-auto*—that reflects Vista's new *delayed start* option. The notion of delayed-start services reflects Microsoft's observation that many auto-start services need to start automatically but don't necessarily have to start immediately. Microsoft wanted Vista to get started up and ready to go as quickly as possible, and part of the reason why the XP and Windows 2000 desktop OSs boot slowly is because they're waiting for those auto-start services that always start immediately.

Other useful options for the SC Config command are *password, error, depend,* and perhaps *obj*. You're already familiar with the obj and password options. A couple months ago, I showed you how to use them for creating a new service: obj= lets you configure which account to run a service under with SC Config just as the obj= parameter lets you specify the service account in SC Create. You probably won't change service accounts very often, but you might end up changing those accounts' passwords, and for that task, you can use the password= option. If a service with a key name of *myservice* has a service account whose password has changed to *swordfish*, you can inform Windows as follows:

```
sc config myservice password= swordfish
```

You can use the error= option to control Windows' behavior when a service fails. Remember, while creating a new Windows service, you can tell Windows to respond to a service failure in one of four ways: *ignore*, which merely notes the failure in the event log; *normal*, which acknowledges the failure with a message but lets operations continue; *severe*, which reboots the system with Last Known Good and tries again; or *critical*, which reboots the system, retries the service, and—if it still fails to run—bluescreens the system. I can tell Windows that if *myservice* doesn't run, Windows doesn't run (clearly a measure to use sparingly), as follows:

```
sc config myservice error= critical
```

We're not quite done with SC Config—there's one more oddity to look at. Over the course of the past three columns, I've shown you that whenever SC lets you specify more than one option/value pair for a command, you separate those option/value pairs with forward slashes. I demonstrated the technique last month with the depend= option, and you can also observe it if you look up the syntax of Vista's SC command. By contrast, with SC Config, you specify more than one option by merely separating them with spaces. (Granted, this behavior might be considered standard in the scripting world; it just seems odd in the context of SC's other syntax.) For example, to combine those last two commands into one, I could type

```
sc config myservice password= swordfish error= critical
```

Consider the Possibilities

Need to control a service from the command line because you want to use a batch file? Want to use a low-bandwidth textual interface for remotely configuring a system? Perhaps you're just getting up to speed with the command line so that you can control the upcoming command-line-only Server Core product. Whatever your scenario, you'll find SC a useful tool.

InstantDoc ID 94722

Tips for Virtual Server 2005 R2

Get the most out of your VMs

Virtualization is a hot technology, and for good reason. Today's virtualization products are mature, production-ready, and can be used to solve many problems that businesses face today. Here are 10 tips for using Microsoft Virtual Server 2005 Release 2 (R2) more effectively.

1 Upgrade to Virtual Server 2005 R2—First, upgrade to Virtual Server 2005 R2. Virtual Server 2005 R2 offers many new features, including 64-bit host support, support for Windows clustering services, new support for popular Linux distributions, fixed hyper-threading, and performance improvements of as much as 100 percent for Microsoft SQL Server and Exchange Server.

2 Allocate enough memory for your VMs—Memory is an important factor to consider when creating new virtual machines (VMs). When you size a VM, remember it will require at least the same amount of memory as the physical machine plus an additional 32MB for VM overhead. So, to adequately move a 512MB system to a VM you'd need to allocate 544MB of RAM.

3 Allocate enough memory for the host—Although it's vital to allocate enough memory for your VMs, it's even more important that you reserve adequate memory for the host. If the host runs out of memory and begins paging, the performance of all the VMs will suffer. 512MB should be considered the minimum amount necessary for the host. Running Virtual Server 2005 R2 on an x64 platform boosts the available memory as the supported system memory jumps from a 4GB maximum on the 32-bit platform to 1TB on the x64 platform.

4 Install Virtual Machine Additions—Microsoft Virtual Machine Additions is a component for improving VM performance and usability. Virtual Machine Additions provides high-performance mouse and video support by moving some important VM functions into the system kernel and enables optional host time synchronization.

5 Create your VHDs on a separate disk—VMs must share host resources, and the hard disk resource greatly affects performance. You'll reduce system resource contention and improve overall performance by creating Virtual Hard Disks (VHDs) on separate disk drives and even separating VM controllers from the drives and controllers that the host OS uses.

6 Use differencing disks to save disk space—You'll find that VMs and their associated VHDs can take up a lot of space. Using Virtual Server 2005 R2's differencing disks can significantly reduce the host storage requirements. Differencing disks enable you to create a read-only parent disk image that can provide the base for multiple other VMs, which saves a lot of host storage.

7 Remove VHDs from antivirus scanning—Antivirus scanning can drag down VM performance, so remove your VM's VHDs from antivirus scanning. This includes your .vhd, .vmc (VM configuration), .vud (undo disk), and .vsv (saved-state) files. Also, don't create your VHDs on encrypted or compressed volumes.

8 Open port 1024 for remote management—Unlike desktop-oriented VM products—which you typically manage via a Windows GUI—you manage Virtual Server 2005 R2 by using a Web interface, facilitating remote management of the server. By default, Virtual Server 2005 R2 uses port 1024 for the management console and port 5900 for the Virtual Machine Remote Control (VMRC) client. The VMRC client also uses ports 137 and 138 if Kerberos is in use.

9 Configure automatic VM startup—You usually want VMs to automatically start whenever the host system starts if your servers are consolidated. To configure automatic startup, open the Virtual Server Administration Web site, select the VM that you want to automatically start, and click Configure. Then, select General Properties and in the *Action when Virtual Server Starts* drop-down menu select *Always automatically turn on virtual machine*.

10 Take advantage of Windows 2003 R2 virtualization licensing—One VM-technology gotcha is that the OS used in a guest must be licensed as if it were running on a physical device. Windows Server 2003 Release 2 (R2), Enterprise Edition and Windows 2003 R2, Datacenter Edition provide a more cost-effective model for licensing Windows Server instances running in VMs. Windows 2003 R2 Enterprise allows as many as four active Windows Server instances, and Windows 2003 R2 Datacenter allows an unlimited number of active Windows Server instances.

InstantDoc ID 94289

Michael Otey
(mikeo@windowsitpro.com) is technical director for *Windows IT Pro* and *SQL Server Magazine* and president of TECA, a software-development and consulting company in Portland, Oregon. He is the author of *SQL Server 2005 New Features* (Osborne/McGraw-Hill).


HOW WELL ARE YOUR
SERVERS PROTECTED?

Blake Eno (beno@windowsitpro.com)
is product editor for *Windows IT Pro* and *SQL Server Magazine*.

At a Glance

Readers Review HOT PRODUCTS

—Carlton Whitmore, systems analyst

Reader:
Carlton Whitmore
Systems analyst
Product:
Formatta E-Forms Suite
Company:
Formatta
Contact:
www.formatta.com

Online Forms Made Easy

Formatta E-Forms Suite

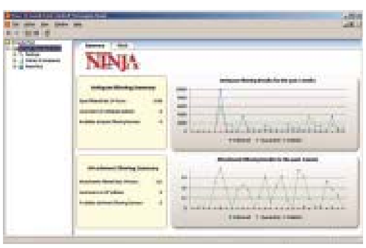
With 15 remote offices, my company was wasting a lot of time, money, and paper on internal request forms. Each office was required to send check requests, vacation requests, and so on, to our home office in Austin, Texas. We needed an online forms solution that could streamline this process and offer some of the components that other solutions lacked, such as a way for users to sign documents, track versions of a form, and export data into Excel and SQL Server. We decided on **Formatta** E-Forms Suite, which bundles four components—the Formatta E-Forms Manager, Formatta Filler, Formatta Server, and Formatta Designer 7.0—into one package.

E-Forms Manager lets our IT staff update existing forms, and when a user signs an updated form, previously downloaded forms are automatically updated. This is a huge time-saver when you have over 130 users and document versions floating around. The solution also integrates nicely with our existing Active Directory environment, which eliminates having to create additional security for end users. You can also use LDAP or Formatta's own authentication. The Server component encrypts the signing process, and this means I don't have to use SSL when I publish forms. The Designer component lets me import existing PDF forms or create new ones and convert them to online forms, with minimal modifications. I've been looking for a solution like this for two years, and Formatta is the only vendor that provides everything I need in one package.

What's Hot continues on page 84

SUNBELT MESSAGING NINJA™ for Exchange

Meet Sunbelt Messaging Ninja—The new all-in-one, best-of-breed, third-generation messaging security solution: Ninja is a plug-in framework that integrates best-of-breed antispam, antivirus, and SMART attachment filtering on your Exchange server. **Much easier to manage:** Ninja was designed by admins for admins. Its MMC interface is a breeze so you can get up and running in minutes vs. hours. **Better multi-engine spam detection:** Ninja's spam filtering decimates junk mail with both Cloudmark (which includes anti-phishing) and Sunbelt's own heuristics-based iHateSpam engines. And, of course, it also supports RBLs and SPF. **Integrated multi-engine antivirus:** Ninja combines the power of multiple high-quality AV engines. **Great end-user control:** The policy-based plug-in architecture allows you powerful, granular control. You can finally rule with an iron fist. **SMART attachment filtering:** Ninja features the first flexible policy-based attachment filter that isn't fooled by extensions. It looks *inside* files to determine their true identity. Your policies decide what happens to all attachments.



WindowsITPro READERS CHOICE 2006 Winner

Eval at www.sunbelt-software.com/ninjawinb.

Sunbelt Software

Email sales@sunbelt-software.com or call 888-688-8457 for your competitive upgrade quote

Sunbelt Software Tel: 1-888-688-8457 or 1-727-562-0101 Fax: 1-727-562-5199 www.sunbelt-software.com sales@sunbelt-software.com

The competitive upgrade is based on 50% of Ninja list price.

better with 1&1!

center offers you more power, more security, more value!

More Power!

	1&1 BUSINESS	Yahoo! STANDARD	Go Daddy PREMIUM
Included Domains	3	1	$1.99/year with purchase
Web Space	250 GB	10 GB	200 GB
Monthly Transfer Volume	2,500 GB	400 GB	2,000 GB
E-mail Accounts	2,500 IMAP or POP3	500 POP3	2,000 POP3
Mailbox Size	2 GB	2 GB	10 MB
Search Engine Submission	✓	✓	Extra charge applies
Website Builder	18 Pages	✓	Freeware
Flash Site Builder	18 Pages	–	–
Photo Gallery	✓	✓	✓
RSS Feed Creator	✓	–	$4.99/month
Blog	✓	✓	Freeware
Map & Driving Directions	✓	✓	–
Dynamic Web Content	✓	✓	–
Web Statistics	✓	✓	✓
E-mail Newsletter Tool	✓	$10/month	$3.99/month
In2site Live Dialogue	✓	–	–
Chat Channels	✓	–	✓
Form Builder	✓	✓	–
Premium Software Suite	✓	–	–
90-Day Money Back Guarantee	✓	–	–
Support	24/7 Toll-free Phone, E-mail	24/7 Toll-free Phone, E-mail	24/7 Phone, E-mail
Price Per Month	$9.99	$19.95	$14.99

We offer a variety of hosting packages to fit your needs and budget.

or visit us now **1and1.com**

1&1

Connect to Remote Computers Behind a Firewall

NetworkStreaming's SupportDesk Appliance 300

Reader:
Asif Shaikh
Senior technical support engineer

Product:
SupportDesk Appliance 300

Company:
NetworkStreaming

Contact:
www.networkstreaming.com

We were looking for a better way for our company's Help desk to provide remote support to our traveling workforce. We ran into difficulties when we had to remotely connect to and fix computers for employees who were connected at client sites behind a firewall, which is a common problem with many remote-support solutions.

Our solution had been to walk users through step-by-step instructions to troubleshoot and fix the problems themselves. But with **NetworkStreaming** SupportDesk Appliance 300, I can connect to any machine that has Internet access and take over the machine quickly. Our users love the product because it makes their lives so much easier. A user can be in a meeting or out to lunch while a support technician accesses his or her computer and solves the problem.

"With NetworkStreaming SupportDesk 300, I can connect to any machine that has Internet access and take over the machine quickly."
—Asif Shaikh, senior technical support engineer

Unlike other products, SupportDesk lets us connect to remote computers even when they're behind a firewall, and it doesn't require us to leave a port open solely for SupportDesk. Additionally, if a connection is lost, SupportDesk automatically reconnects with the support desk technician responsible for that job. Another benefit is that we don't need to preinstall a client on a user's machine. A client is installed while we're connected, and when the session is closed, the client is automatically uninstalled.

What's Hot continues on page 85

A Free Tool That Monitors, Inventories, and Reports on Your Infrastructure

Spiceworks IT Desktop

Reader:
Jonathan Chorney
Systems administrator
Product:
Spiceworks IT Desktop
Company:
Spiceworks
Contact:
www.spiceworks.com

I started using **Spiceworks** IT Desktop when it was still in beta. It's a free tool that provides a remarkably complete view of all devices connected to my network without using any agents. I manage 50 workstations and 14 servers, so I'm a long way from having the budget, manpower, and time that the enterprise-oriented tools require. Spiceworks gives me information on computer hardware configuration; all software, services, and hotfixes on each computer; all connected devices; offline servers; low disk space; plus hardware and software and low-toner alerts. All this information is presented in an interface that's easy to understand. I'm also really impressed with the quality of the support forums and the energy of the moderators whenever I have any questions about the software. This is a great tool for anyone who needs all the basic information on his or her systems without spending a ton of money or time learning a commercial tool. IT Desktop will serve me well into the future.

"This is a great tool for anyone who needs all the basic information on his or her systems."

—Jonathan Chorney, systems administrator

(Editor's note: Spiceworks isn't limited to just a monitoring and inventory solution. The software can run reports for all installed software, trouble tickets, and disk usage. You can use predefined reports or create your own from scratch. All reports can be exported to PDF or Microsoft Office Excel formats.)

What's Hot continues on page 86

Combine Data from Multiple Sources for Troubleshooting Anomalies

Ascendview's WildMetrix

> "WildMetrix can combine data from any source onto 1 time-oriented graph."
>
> —Buzzy Winter, senior certified consultant

Reader: Buzzy Winter
Senior certified consultant

Product: WildMetrix

Company: Ascendview

Contact: www.wildmetrix.com

As a consultant, I've seen my share of products that help troubleshoot anomalies in network infrastructures, and they all have their good points and bad points. But **Ascendview**'s WildMetrix has one thing that no other product I've seen has—the ability to combine data from any source onto one time-oriented graph, including performance counters, event log entries, and SNMP events. One of my clients was having problems with in-house ASP Web applications that would crash and then require restarting Microsoft IIS. Without WildMetrix, I had to use Microsoft's Performance Monitor and wade through the different pieces and was left with nothing to correlate them with. But with WildMetrix, I can take the same performance counter data and correlate that data on the same graph with individual Web page counters and determine what a specific Web page was doing to cause an application to crash. I've also used the software to determine when an Active Directory Group had its membership changed by correlating the security event logs on the domain controllers with service account failures from the system event log.

On one occasion, end users reported intermittent slowness with Exchange Server. WildMetrix was able to correlate event logs and system counters to determine that several antivirus and defragmentation runs were running simultaneously, which caused a low level of free RAM for the server. Without WildMetrix, seeing all of this would have been nearly impossible.

InstantDoc ID 94598

DIRECTORY OF SERVICES

Windows IT Pro Network

Search our network of sites dedicated to hands-on technical information for IT professionals.
http://www.windowsitpro.com

Support

Join our discussion forums. Post your questions and get advice from authors, vendors, and other IT professionals.
http://www.windowsitpro.com/forums

News

Check out the current news and information about Microsoft Windows technologies.
http://www.wininformant.com

EMAIL NEWSLETTERS

Get free NT/2000/XP/2003 news, commentary, and tips delivered automatically to your desktop.

- *Windows IT Pro UPDATE*
- *Windows Client UPDATE*
- *Windows Tips & Tricks UPDATE*
- *WinInfo Daily UPDATE*
- *Developer UPDATE*
- *Exchange & Outlook UPDATE*
- *Scripting Central*
- *Security UPDATE*
- *SQL Server 2005 Express UPDATE*
- *SQL Server Magazine UPDATE*
- *Storage UPDATE*
- *Windows IT Library UPDATE*
- *Connected Home EXPRESS*

http://www.windowsitpro.com/email

TECHNICAL NEWSLETTERS

Exchange & Outlook Administrator

Discover smart solutions for Exchange and Outlook administrators.
http://www.windowsitpro.com/microsoftexchangeoutlook

Windows Scripting Solutions

Learn how to create more powerful scripts and get tips for automating those tedious administrative tasks.
http://www.windowsitpro.com/windowsscripting

Windows IT Security

Discover practical, how-to advice for avoiding and solving security problems.
http://www.windowsitpro.com/windowssecurity

RELATED PRODUCTS

Custom Reprint Services

Order reprints of *Windows IT Pro* articles. Contact Michael Dudziak at mdudziak@penton.com.

Super CD/VIP

Get exclusive access to all of our print publications, including *Windows IT Pro,* via the new, banner-free VIP Web site.
http://www.windowsitpro.com/sub/vip

Article Archive CD

Access every article ever printed in *Windows IT Pro* magazine since September 1995 with this portable and speedy tool.
http://www.windowsitpro.com/sub/cd

SQL SERVER MAGAZINE

Explore the hottest new features of SQL Server, and discover practical tips and tools.
http://www.sqlmag.com

Ad Index

For detailed information about products in this issue of Windows IT Pro, visit the Web sites listed below.

VENDOR DIRECTORY

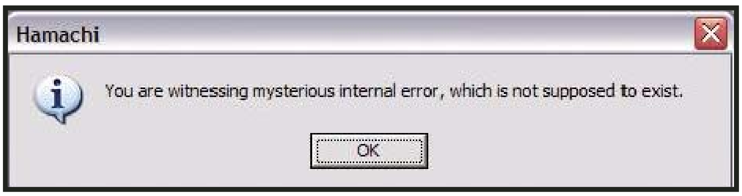
The following vendors or their products are mentioned in this issue of *Windows IT Pro* on the pages listed below.

Send your funny screen shots, juicy rumors, or industry humor to rumors@windowsitpro.com. If we use your submission, you'll receive a Ctrl+Alt+Del coffee mug.

LOST IN TRANSLATION

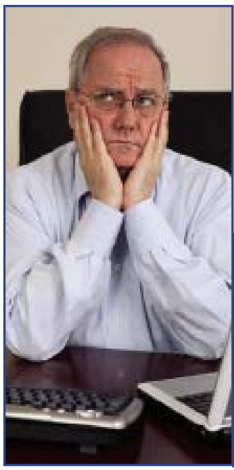
The shame of the installation

Disturbing the Tao



Like Father Like Son

Allow us to introduce you to John Cramer and his son Ethan. Young Ethan looks forward to the day when he'll have his very own subscription to *Windows IT Pro*. Would you like to share a photo of your IT-leaning child? Send your cute pics to rumors@windowsitpro.com.

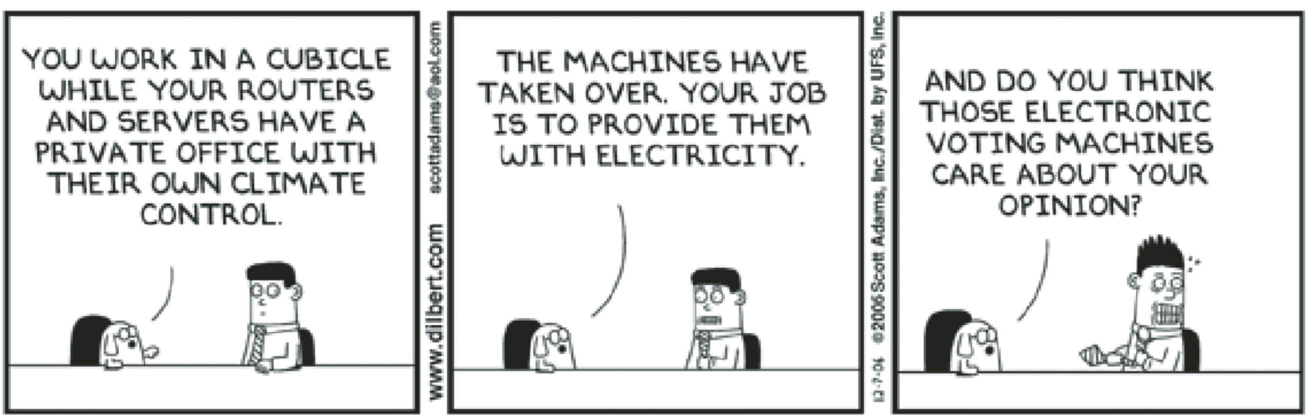


User Moment of the Month

I recently diagnosed a keyboard problem as a faulty port on the user's PC. Rather than replace the computer's main board, I decided to send the user a new keyboard that supports USB connectivity. To my surprise, the user was angry when the new keyboard arrived. I assured him that the replacement keyboard would work just fine and asked why he was disappointed with the solution. He said, "Why are you making me change my keyboard? Now I'll lose all my stored passwords!"

—*Brent Sodders*

DILBERT® by Scott Adams



February 2007 issue no. 150, *Windows IT Pro* (ISSN 1552-3136) is published monthly. Copyright 2007, Penton Media, Inc., all rights reserved. Subscriptions in US, $49.95 for one year; in Canada, $59 US currency, plus 7% for GST for one year; in UK £59; in all other countries, US $99. Windows is a trademark or registered trademark of Microsoft Corporation in the United States and/or other countries, and *Windows IT Pro* is used under license from owner. *Windows IT Pro* is an independent publication not affiliated with Microsoft Corporation. Microsoft Corporation is not responsible in any way for the editorial policy or other contents of the publication. *Windows IT Pro,* 221 E. 29th St., Loveland, CO 80538, (800) 793-5697 or (970) 203-2782. Sales and Marketing Offices: 221 E. 29th St., Loveland, CO 80538. Advertising rates furnished upon request. Periodicals Class postage paid at Loveland, Colorado, and additional mailing offices. **POSTMASTER: Send address changes to *Windows IT Pro,* P.O. Box 447, Loveland, CO 80539-0447. SUBSCRIBERS:** Send all inquiries, payments, and address changes to *Windows IT Pro,* Circulation Department, P.O. Box 447, Loveland, CO 80539-0447. Printed in the USA. BPA Worldwide Membership Applied for May 2006. Ride-Along Enclosed.

Introducing

PerfectDisk 8 — EVERYTHING FASTER.

- Centralized Management And Reporting
- Patent-pending Resource Saver™ Technology
- Exclusive Space Restoration™ Technology
- Exclusive AutoPilot Scheduling™

Recognized as the world's most powerful defragmenter, PerfectDisk has always been the secret to faster, more reliable computers. Now, with a powerful new suite of enterprise tools, PerfectDisk 8.0 takes disk defragmentation to the farthest reaches of the enterprise, while placing total control right at your fingertips.

Are you sitting down? Good. Because with the PerfectDisk Command Center™ you can easily deploy, configure and manage the defragmentation of every system on the enterprise... all from the comfort of your own desktop. And that's just the beginning.

Our all new enterprise reports deliver valuable performance statistics and at-a-glance graphical displays that track and identify any fragmentation issue on any managed computer, and much more.

In addition, PerfectDisk's patent-pending Resource Saver™ technology finds file fragmentation without having to first open the file, further reducing any system impact of defragmentation. And new disk and CPU throttling provide even greater control over resources.

What's more, Raxco's exclusive AutoPilot Scheduling™ provides automatic defragmentation at the optimal time for each user. And AutoPilot Scheduling's Screen Saver Mode enables idle-time defragging at user-defined intervals. (There's really nothing to it.)

And features like our Single File Defrag and Consolidate Free Space Defrag (part of PerfectDisk's Space Restoration Technology™) are particularly valuable for users working with supersize files.

Give your users reason to stand up and cheer. And while PerfectDisk 8.0 is busy keeping each computer in tip top shape, you can sit back and simply take the credit. For the details and a free demo, visit

www.pdcommandcenter.com

RAXCO SOFTWARE

1-800-546-9728
www.raxco.com

Certified for Microsoft® Windows Server™ 2003 Standard Edition

Microsoft GOLD CERTIFIED Partner

Designed for Microsoft® Windows® XP Windows® 2000

PC MAGAZINE EDITORS' CHOICE June 8, 2004 PerfectDisk 6.0

PC MAGAZINE EDITORS' CHOICE May 24, 2005 PerfectDisk 7.0

Hungry for a better Desktop Management Solution?

Get your fill with ScriptLogic's Desktop Authority.

DESKTOP AUTHORITY®

Download a 30-day trial today and get a FREE Fortune Cookie T-Shirt.

Download a 30-day trial today at www.ScriptLogic.com/menu

SCRIPTLOGIC®

Point, Click, Done!